Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club

er
nnlich sind
inante jun-
Spaß an ta-

Tyrannin.
lseitig und
zu schät-

Dildos, Peitsche, High-Heels, Erziehung). Bei Sympathie sollte es mehr als nur ein Treffen sein. Diskretion ist Ehrensache. Chiffre 06/488

Frustrierte Telekommmitarbeiterin sucht devoten Herrn zum Abreagieren. Chiffre 06/389

ISSN 0930-1045 August 1996 Nr. 55 DM 5,00 Postvertriebsstück C11301F

Impressum

Die Datenschleuder Nr. 55, August 1996

Herausgeber:
Chaos Computer Club e.V., mail@ccc.de
Schwenckestr. 85, D-20255 Hamburg
Tel 040 - 401 801 - 0, Fax 040 - 491 76 89

Redaktion :

Redaktion Datenschleuder, ds@ccc.de
Neue Schönhauser Str. 20, D-10178 Berlin
Tel 030- 283 54 87 2, Fax 030- 283 54 87 8

ViSdP: Andy Müller-Maguhn

Druck: St. Pauli Druckerei, Hamburg

Mitarbeiter dieser Ausgabe
Amok *(amok@ccchh.ccc.de)*, Christine *(c.schoenfeld@bionic.zerberus.de)*, Bishop *(bishop@ccc.de)*, Fiedel *(fiedel@kadewe.artcom.de)*, Frank Rieger *(frank@ccc.de)*, Andy Müller-Maguhn *(andy@ccc.de)*, Jens Ohlig *(j.ohlig@bionic.zerberus.de)*, Wau Holland *(wau@ccc.de)*

Mitglieder des CCCe.V. erhalten die Datenschleuder im Rahmen Ihrer Mitgliedschaft.

Das Titelbild ist keine Eigenschöpfung sondern der Rubrik „Lust & Liebe: Harte Welle" der Berliner Zeitschrift Zitty, Ausgabe 6/96 entnommen.

Eigentumsvorbehalt:
Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden.

(Gast-)Editorial

Bishops' Worte aus Leibzsch

Montag

In einer Sendung des Mitteldeutschen Rundfunks, "Umschau" steht eine telekomgebeutelte Familie vor der Kamera. Das ältere Ehepaar legt eine Hand auf das Telefonbuch, die andere erhebt es zum Schwur: "Nein, wir haben diese Telefonrechnung von 16.000,- DM nicht verursacht", schwören die beiden T-Abgezockten mit Tränen in den Augen. Ich erkenne anhand der gelben Farbe, daß es sich bei dem Telefonbuch um das alte Testament halten muß.

Dienstag

Mein E-Mail-Briefkasten war heute mit 250 Nachrichten übervoll, obwohl gestern erst geleert und bearbeitet. Da liegt ein Fehler vor. Ich schreibe an den Support meines E-Mailanbieters "ultranet.de".

Er antwortet: "Sie haben Mail an einen Empfänger meier@ultranet.com geschickt. Nachrichten an den Domain-Namen "ultranet.com" werden an die ULTRA geschickt. Dort ist der Empfänger meier@ultranet.com" nicht bekannt. Da der Absender ein lokaler User "Bishop@ultra.ultranet.de" ist, wird die Nachricht dennoch entgegen genommen und ins Internet geschickt. Von dort kommt die Nachricht zur ULTRA mit dem hier nicht bekannten Empfänger "meier@ultranet.com". Da der Absender ein lokaler User "Bishop@ultra.ultranet.de" ist, wird die Nachricht dennoch entgegen genommen und ins Internet geschickt. Von dort kommt die Nachricht zur ULTRA mit dem hier nicht bekannten Empfänger "meier@ultranet.com". Da der Absender ein lokaler User "Bishop@ultra.ultranet.de" ist, wird die Nachricht dennoch entgegen genommen und ins Internet geschickt.

..... Da die Nachricht immer wieder erfolgreich ins Internet verschickt werden konnte, haben Sie jedesmal eine Service-Postmaster-Meldung erhalten und Ihr Briefkasten ist übervoll. Leeren Sie mal regelmäßig Ihre Post!"

Ich blicks' da nicht mehr durch, Kommunikation ist ungeheuer kompliziert geworden. Steckt da der BND hinter?

Mittwoch

Ich glaub, mich tritt ein "Falcon": Morgens um 8:12 Uhr hebe ich 100.- DM mit meiner EC-Karte am Automaten ab. Nachmittags gegen 14:16 Uhr kaufe ich bei Karstadt im dritten Stock mit der EC-Karte ein Mousepad für 12,95 DM. Wenige Minuten später will ich ein Stockwerk tiefer Hosenträger für 15,95 DM mit der EC-Karte erwerben. Die Kasse streikt, die Verkäuferin will meinen Perso sehen. In der Menschenschlange böse Blicke: "Wennse ihr Gondo ieberzochen haben, solldn se geene Hosendräscher goofn", raunt mir ein Sachse zu. Peinlich. Die Verkäuferin entschuldigt sich: "Ein neues System." Was mag sich das neuronale Netz bei der GZS gedacht haben? Warum hebt der Typ einen Hunni bar ab und kauft später einen "Maustebbisch" und dann "Hosendräscher" mit Karte?

Donnerstag

Ein Berliner Stadtmagazin muß einem Kollegen nach einem Gerichtsbeschluß 15.000.- DM zahlen, weil sie ihn versehentlich falsch zitiert hatten: "Ficken, ficken, ficken und nicht an die Leser denken". Im CCC wird natürlich weniger an Sex gedacht: "Applets, applets, applets und an die User denken!".

Freitag

Telefonat mit einem Hamburger Hacker. Er hat zuviel Wilson gelesen. Ich versuche ihn mit etwas Realität zu trösten. Abends lese ich Wilson, "Der neue Prometheus" (ISBN 3-499-18350-1). Was ist schon Realität. Ich glaub, ich träume. Einige Stunden später: Anruf eines Berliner Hackers. Er glaubt, er sei Gott. Ich glaub', ich spinne. Ich glaub', Realität wird nie wieder, was sie mal war. Was ist eigentlich Realität? Es wird Zeit, daß die neue Hackerbibel erscheint...!

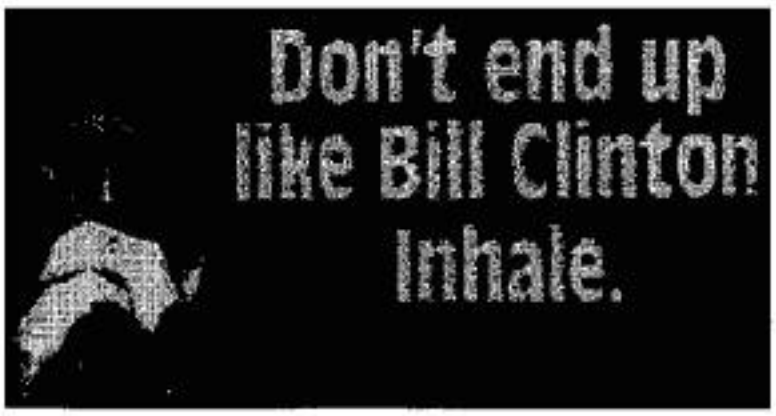
Samstag

Es läuft ein Werbespot der Telekom: "Im Zeichen der T-Aktie". Dabei erheben alle "User" brav die Hände zum T-Schwur (Nein, es ist kein verbotener Gruß, auch Polizisten nehmen daran teil !). Sie haben aber nicht gemerkt, daß es das Sportzeichen zur "Auszeit im Basket- oder Volleyball ist.

Arme Telekom - Jetzt wirbt sie schon für Bedenkzeit im harten Marktwettbewerb übers Fernsehen. Ob das hilft?

Sonntag

Ein Telekomiker zeigt mir voller Stolz seinen "T-Monitor vor Ort", eine Art regionale BILD für Telekomiker, nur nicht öffentlich. Darin steht, daß die Angestellten nix zu Journalisten über ihre Aktienbeteiligung sagen dürfen: "Wir einigen uns auf einen anderen Sprachgebrauch ...". und: "Es könnten ja Schlagzeilen dadurch produziert werden". Dann der Hammer: Die Süddeutsche druckte am 11. Juni einen Artikel, in dem über einen Holländer berichtet wurde, der wegen seiner Internet-Sucht eine Drogenberatungsstelle aufsuchte. Skandalös! Muß nun der Telekom-Vorstand wegen Drogenhandels verhaftet werden ?...



I n d e x

Impressum	02
Editorial	02
Index (das hier)	03
Vorauseilend gehorsam: Netzzensur	04
Chaos Realitäts Dienst: Kurzmeldungen	05
Besuch bei der Telekom	08
Anis-Bug: Zusammenfassung	10
Chipkartenmodule-Übersicht	11
EWSD-DIV Leistungsmerkmale	12
Kryptisches von der NSA	14
Hackers of planet earth: Argentinien	15
Aus der Postbearbeitung	16
Das Jahr 00	18
Agenten: Vertrauen gut, Kontrolle besser	19
Agenten: Quellverweise	21
Elektropost	22
Techno-Terrorismus?	23
Buchbesprechung:"Die Datenmafia"	25
Kopflastige Ermittlungen	26
Sicherheitssimulation	28
Das letzte	29
Nachruf	30
Adressen	31
CCC e.V. Info / Bestellfetzen	32

Vorrausseilend gehorsam

Neue Ideen zur Einschränkung von Inhalten im Netz

"Ich begrüße die Initiative der der deutschen Online-Wirtschaft, einen Internet Medienrat als Gremium freiwilliger Selbstkontrolle einzurichten", freute sich Wirtschaftsminister Rexroth Anfang Juni. Endlich ist alles wieder gut. Das Internet wird kontrolliert und Straftaten kann es theoretisch nicht mehr geben.

"Die vier apokaplyptischen Reiter der Netze" (padeluun@bionic.zerberus.de), die das Internet in Presse, Funk und Fernsehen bekannt machten, also Kinderpornographie, Faschopropaganda, Organisierte Kriminalität und Drogenverherrlichung, dürften in Zukunft nicht mehr reiten. Zu lange hatten sie den warmen Guß an Cyberdollars aus dem Sprühkopf des Internet-Brausers verhindert und deutsche Internetprovider in die Ratlosigkeit getrieben.

Wenn man nicht mehr weiter weiß, gründet man einen Arbeitskreis; eine sogenannte "Internet Content Task Force" wird sich in Zukunft um die Einhaltung der Gesetze im Netz kümmern. Mit der Unterstützung praktisch aller Internetprovider in Deutschland wird man in Zukunft am DE-CIX, dem deutschen Knotenpunkt für den kommerziellen Internetaustausch zensieren, redigieren und verfolgen: "Die ICTF wird die vorhandenen Informationen über die Herkunft von News erfassen [...], daß auch nachträglich noch ermittelt werden kann, wer einen Artikel verschickt oder wer die Identität des wahren Autors verschleiert hat. [...] Weiterhin werden die vorhandenen oder neu eingerichteten Newsgroups klassifiziert, so daß Gruppen, die ausschließlich oder überwiegend der Verbreitung rechtswiedriger Informationen dienen, von der weiteren Distribution ausgeschlossen werden können." Weiterhin will man durch Cancel-Nachrichten einzelne Artikel nachträglich aus dem Usenet entfernen.

Mit der selbsternannten "Internet Content Task Force" besteht zum ersten Mal eine Zensurstelle im Internet. Nachdem die ICTF Newsgroups als den "augenblicklich wohl kritischsten Teil des Internet" erkannt hat, wird sie jetzt ihre Arbeit dort aufnehmen. Natürlich wendet man sich in der Pressemeldung vom 5. Juni ausdrücklich gegen "Zensur" — eine staatliche Zensur ist nicht erwünscht und soll durch die Initiative der Wirtschaft verhindert werden.

Das Verhalten, das hier die deutschen Internetprovider (namentlich CERFnet, ECRC, EUnet, GTN/Contrib, ipf.net, IS/Thyssen [vormals MAZ], Point of Presence, nacamar, NTG/XLink, roka, seicon und spacenet) an den Tag legen, läßt den Internetbenutzer im besten Fall fassungslos reagieren. Weder wird hier bedacht, daß man mit solchen Methoden, um Rechtssicherheit im Netz (die ICTF spricht hier voller Stolz sogar von "law & order") zu schaffen, Ärger auf sich zieht und Netzgepflogenheiten verletzt, noch scheint es den Providern bekannt zu sein, daß ihnen trotz ihrer Marktmacht (schon nachgesehen, ob Dein Provider auch zensiert?) die Inhalte im Netz nicht gehören. Ein Artikel gehört eben dem Autor oder der Autorin, keiner "Internet Content Task Force".

Hier gilt es neue Strukturen zu schaffen. Wir brauchen Newsversorgungen, die von DE-CIX unabhängig laufen und den Zensurwahn der ICTF nicht mitmachen. Der aus der niederländischen Hackergruppe Hacktic hervorgegangene Provider XS4ALL hat sich schon bereit erklärt, hier an einer technischen Lösung gegen den deutschen vorauseilenden Gehorsam mitzuwirken.

Aber die apokalyptischen Reiter haben auch an einer anderen Stelle zugeschlagen: Um die Verbreitung von Sexbildchen im Netz zu verhindern gibt es jetzt PICS.

PICS steht für "Platform for Internet Content Selection" und soll die Welt (vor allem das WeltenWeite Weben) ein Stück sauberer und amerikanischer machen.

Mit vorinstallierten "Webweltbildern" (iX 7/96), die Einstellungen in den Rubriken "Sex", "Gewalt", "Nacktheit" und "rüde Sprache" beinhalten, soll der Nachwuchs bestimmte Seiten im WWW nicht mehr besuchen können. PICS wird als die Lösung aller internetbezogenen Erziehungsprobleme propagiert.

Tatsächlich dürfte hier amerikanische Prüderie zur technischen Norm werden, denn vorgestellt und von Firmen wie AOL Bertelsmann Online umjubelt wurde PICS auf der 5. WWW-Konferenz in Paris. Die Einordnung in die vier seltsam beschränkten Rubriken soll vom WWW-Anbieter selbst kommen. Wer sich weigert, eine Selbsteinschätzung nach den PICS-Kriterien vorzunehmen, der kann von Minderjährigen einfach nicht mehr "angesurft" (so heißt es wohl im Marketingdeutsch) werden.

Angst vor Neuem, Inkompetenz und Machtwahn auf der ganzen Linie also.

Wir befinden uns in einem Internet, in dem Firmen die anscheinend gewonnene Vorherrschaft nun gegen den Staat verteidigen. Da man aber eher an Profit als an dem Menschenrecht auf Kommunikation und Information interessiert ist, wehrt man sich gegen die böse staatliche Zensur mit freier, marktwirtschaftlicher Zensur. Längst gehören die Netze nicht mehr jenen, die drin leben.

Willkommen in der Marktwirtschaft.

j.ohlig@bionic.zerberus.de

Indianer-Definitonen:

Windows-Benutzer:
Weisser Mann sitzt vor Sanduhr

Medien-Benutzer:
GeistigesWesen, nicht Datenschatten

Chaos Realitäts Dienst

„T" CD-ROM umsonst

(crd/23.06.1996) Bei der Telekom kann unter der Faxnummer 0130 - 800 104 kostenlos eine CD-ROM mit dem Diensteangebot des Unternehmens angefordert werden...

Telefonische Wasseranforderung

(crd/23.06.1996) Bisher unbestätigten Gerüchten zufolge weigern sich Versicherungen von Kaufhäusern neuerdings, diese gegen Wasserschäden zu versichern solange sie ihren Kunden die Benutzung von Mobiltelefonen nicht untersagen.

Hintergrund sind offenbar Fälle, in denen im Kaufhaus benutzte Mobiltelefone die Sprinkleranlage ausgelößt haben. Von wegen elektromagnetische Verträglichkeit...

Position im Telekom-Aufsichtsrat = Lizenz zum Gelddrucken?

(dpa/blnz/crd/23.06.96) - Über die Gründe für den Ausschluß von Rolf-Dieter Leister aus dem Aufsichtsrat der Telekom zum 1. Juli gibt es verschiedene Darstellungen.

Zunächst war von „persönlichen Gründen" die Rede, die Leister dazu bewegt haben sollen, von sich aus den Posten zu räumen.

Ein vorab verbreiteter Bericht der „Berliner Zeitung" dokumentierte anonyme Vorwürfe, nach denen er sein Amt aufgrund von mißbräuchlicher Betätigung habe räumen müssen. So ist dort davon die Rede, er habe nicht nur Reisen und Telefonate auf Kosten der Telekom abgerechnet, sondern vor allem Einfluß auf die Vergabe von Aufträgen genommen - im Zusammenhang mit einem Beraterverhältniss mit Siemens.

Die Telekom erklärte, der Bericht sei „in allen relevanten Passagen unwahr" und ein Gutachten der Wirtschaftsprüfungsgesellschaft KPMG habe Leister entlastet; „Herr Leister hat nach eingehender Prüfung der KPMG während seiner gesamten Amtszeit nachweislich nie Einfluß auf die Vergabeentscheidungen der Telekom genommen".

Die „Berliner Zeitung" stellt dies anders dar. Der anonyme Vorwurf, Leister habe Telekommunikationskosten auf die Telekom abgewälzt, sei von KPMG nicht entkräftet worden, schreibt die Zeitung. Den Vorwurf, Leister habe Informationen aus der Planung der Telekom an Konkurrenten und Zulieferer gegeben, habe KPMG nicht geprüft. Die Telekom kündigte an, sie werde „mit allen zu Gebote stehenden rechtlichen Mitteln gegen Urheber und Verbreiter der falschen Behauptungen vorgehen".

In einer Anhörung des Bundestag-Ausschusses für Post und Telekommunikation wurde die Rolle von Gutachten vor einiger Zeit folgendermaßen beschrieben: „Mit Gutachten ist es wie mit der Liebe. Wenn man dafür bezahlt, verändern sie den Charakter."

American Express verkauft seine Kunden

(cw/cid/crd/06.96) - American Express hat bekannt gegeben, nunmehr mit der Vermarktung der persönlichen Daten und Personenprofile ihrer 40 Millionen Kunden ein neues Geschäftssegment zu eröffnen. Wie der Vizechef des Konzerns, Barry Hill, bekanntgab sollen nicht Kreditkarten länger das Kerngeschäft ausmachen, sondern die Vermarktung von zielgruppengerechten Daten an interessierte Unternehmen aus Werbung, dem Versicherungswesen, der Tourismusbranche oder dem Versandhandel.

Etwa 10.000 verschiedene Möglichkeiten pro Kartennummer, Informationen über Konsumgewohnheiten des Kunden zu speichern und abzufragen, ermöglicht laut „Computerwoche" inzwischen ein neuronales Computernetz bei American Express.

NTFSDOS erledigt NT-Sicherheit

(pcw/crd) - Eigentlich war das Shareware-Programm NTFSDOS dafür gedacht, NTFS-Partitionen unter DOS bedienen zu können, wenn Windows NT nicht vorhanden ist. Wenn man einen NT-Rechner mit einer DOS-Bootdiskette mit NTFSDOS hochfährt kann man allerdings auch die gegen Lesen geschützten Dateien der NT-Partition lesen - das NT-Sicherheitsbit wird ignoriert. Zu finden: sonstwo.

Global Positioning System bald am Ende?

(crd) Das Global Positioning System (GPS), welches eine Standortpeilung durch den Empfang mehrerer Satellitensignale ermöglicht, ist möglicherweise kurz vor dem Ende.

Denn bei der Konstruktion des Systems wurde die Datumsangabe mit einem 10 Bit Zähler für die Anzahl der Woche versehen; dass heisst, dass nach 1023 Wochen Schluss ist. Die Endgeräte werden daher vorraussichtlich am 22. August 1999 den 6. Januar 1980 anzeigen, so sie denn nicht vorher umgerüstet werden.

Quelle: comp.risc

Analogrufnummernübernahme jetzt

(crd) Die Übernahme der eigenen alten „analogen" (anis, also an digitaler Vermittlung) Rufnummer als MSN (multible subcriber number) für EDSS1 (euro-isdn) ist jetzt ganz offiziell möglich. Offenbar um einen Anreiz gegenüber der Weggefallenen 700.- DM Anlagenförderung zu schaffen haben die neuen EDSS1 Anträge (im Zweifellsfall: nachfragen) der Telekotz ein entsprechendes Feld.

CRD Info Input:
crd@ccc.de

e'schluss?

E-Plus plant Gebühren für SMS

(crd) Aus gewöhnlich gut unterrichteten Kreisen verlautet, dass Netzbetreiber E-Plus plant, ab dem 1. November 1996 eine Gebühr von 15 Pfennig für jede Kurznachricht (SMS) zu Oberechnen.

Auf diese Art und Weise soll die Anschaffung neuer Software für die SMSC (Kurznachrichtenzentralserver) finanziert werden. Abgesehen davon, daß zu diesem Termin dann ein Sonderkündigungsrecht (siehe Kartenvertrag mit E-Plus Service) besteht, planen die gut unterrichteten Kreise diese Entscheidung nicht hinzunehmen - schließlich stellt der umsonst-Kurznachrichtenservice von E-Plus eine der wenigen Telekommunikationsdienstleistungen dar, die der CCC-Forderung nach Nulltarif nachkommt. Auch wäre damit der Betrieb des EGates (www.artcom.de/egate) mindestens stark gefährdet, wenn nicht verunmöglicht.

Falls E-Plus Mobilfunk nicht rechtzeitig einsieht, dass ihnen dann die Kunden weglaufen werden werden entsprechende Protestmittel eingelegt. Infos dazu wird es an den einschlägigen Orten geben.

Quelle: zuverlässig

Siemens setzt auf Internet-Telefonie

(crd/cid/09.04.96) Der Unternehmensbereich „Öffentliche Kommunikationsnetze" der Siemens AG hat angekündigt, Hardware für die Vermittlung von öffentlichen Telefonnetzen mit dem Internet für Telefongespräche auf den Markt zu bringen. In zwei bis vier Jahren soll die Möglichkeit der Internet-Telefonie mit dem Vermittlungssystem namens „Interworking Unit" zur Verfügung stehen.

Quelle: Interview mit dem Leiter des Unternehmensbereichs, Peter Pribilla gegenüber Teletalk

Verfassungsschutz ermittelt

Unsere Verfassung wird auch weiterhin von kompetenten und wachen Beobachtern relevanter Geschehnisse geschützt:

„Informationelle Vernetzung von Rechtsextremisten - Computerspiele :

[...] Indizierte Computerspiele wie „Wolfenstein 3D" oder die Nachfolgespiele „DOOM I" und „DOOM II" wurden auch 1995 angeboten. [...]"

Aus: Verfassungsschutzbericht 1995, S. 180

Telekom ist das allerletzte

Die Telekom ist das allerletzte Unternehmen auf der Beliebtheitsskala deutscher Manager. Dies hat das „manager-magazin" in einer repräsentativen Umfrage unter 2100 Managern der deutschen Wirtschaft ergeben, die „Infratest" durchführte. Unter den 100 größten deutschen Unternehmen glänzt die Telekom mit dem Schlußlicht.

Angesichts dieser Börsengangbedrohlichen Lage empfehlen wir der Telekom die sofortige Einführung des Nulltarifs (zumindest in den Nachtstunden!) um wieder ein positiveres Bild bei den Kunden zu erzeugen. Das Geld für die penetrante Werbung könnte man hier sinnvoller investieren.

Chaos Communication Congress 1996: „Der futurologische Kongress"

Der Chaos Communication Congress 1996 findet unter dem Motto „Der futurologische Kongress - leben nach der Internetdepression" vom 27.-29. Dezember 1996 wieder im Hamburger Eidelstedter Bürgerhaus statt.

Vorschläge für Diskussionsthemen, Workshops und sonstige Eingaben inhaltlicher wie organisatorischer Art nimmt ab sofort der Planungsstab unter congress@ccc.de entgegen.

-t--- oll

Die Telekom-Netzsicherheit lud ein...

Wer unter dieser Überschrift mal wieder einen Bericht über einen Fehler im Telekom-Netz vermutet hat, muß leider enttäuscht werden. Vielmehr geht es um die diplomatischen Beziehungen zwischen dem "Zentrum für Netzsicherheit" der Telekom und dem CCC, namentlich zwischen dem Leiter des Zentrums Herrn Haag und seinen Mitarbeitern auf der einen und Wau Holland und mir (Andy) als Vertreter des CCC auf der anderen Seite.

Die Beziehungen zwischen dieser Abteilung der "T" und dem CCC haben sich, zunächst auf einer Hamburger Veranstaltung, später dann im Rahmen einer Podiumsdiskussion auf dem Chaos Communication Congress 1995 (siehe letzte Datenschleuder) zumindest auf der Ebene der Streitkultur normalisiert. Ende Februar waren wir dann zu einem zweitägigen Besuch beim Netzsicherheitszentrum, bzw. dem Testzentrum der Telekom in Nürnberg eingeladen.

Dabei bekamen wir nicht nur eine Führung durch die Räume der einzelnen technischen Abteilungen, sondern auch von verschiedenen Mitarbeitern ihre Arbeitsbereiche und Alltagsprobleme erklärt. In Nürnberg sind die beiden digitalen Vermittlungssysteme S12 (SEL) und EWSD (Siemens) jeweils einmal im Vollausbau (inkl. Einsatz als S0130-Vst) vorhanden - in einem Raum werden sie dann auf ZZK-Telekom-C7 (zentraler Zechengabekanal...) miteinander verbunden; und es ist tatsächlich ein Mitarbeiter vorhanden, der zwar nur bedingt die deutsche Sprache, aber dafür vollständig C7-ZZK spricht. Übrigens betreibt die Telekom hier sozusagen ein "virtuelles" Ortsnetz (09124) das ausschließlich den Testanlagen vorbehalten ist.

Eines der Dokumente (die wir leider nicht mitnehmen durften) war eine Übersicht über die Softwarefehler und Behebungszeiten der beiden Systeme S12 und EWSD im Vergleich. Erläutert wurde auch die Problematik, mit den Schlußfolgerungen daraus umzugehen; denn obwohl eines der Systeme weniger problembehaftet ist, muß das zweite gehalten werden; nur durch die Konkurrenzsituation der Anbieter sind die Anlagenpreise überhaupt im bezahlbaren Bereich.

Auch die Funktionsweise eines Vermittlungsstellenupdates wurde erläutert. Dabei wird unterschieden zwischen neuen Versionen und den "MODs" (SEL) bzw. "Patches" (Siemens). Eine Updatung erfolgt in der Regel vor Ort (also in der jeweiligen Vermittlungsstelle) - neue Features ("Leistungsmerkmale") schlummern jedoch zunächst und werden im Betriebszentrum fernaktiviert (teils wohl auch zentral; Gebührenumstellungen etc.). Ein Betriebszentrum (früher "RBL" = Regionale Betriebs Lenkung) ist üblicherweise für mehrere DIV'en in einem oder mehreren Rufnummernbereichen zuständig; diese sind teils über Stand-, teils über Modemwählleitungen (ISDN/ANIS-Ports mit GBG-Feature) verbunden - wenn Sie nicht ohnehin im selben Gebäude stehen.

Nach aufgespieltem Backup erfolgt zur Aktivierung (in der Regel nachts) ein Kaltstart; dieser Unterbricht die Gespräche für 2-3 Minuten. Bei Problemen wird sofort das "schlafende" Backup (Rückfallsicherung) aktiviert. Die in den Verträgen zwischen Telekom und Anlagenlieferanten definierte Maximalausfallzeit beträgt 15 Minuten; danach ist eine saftige Vertragsstrafe fällig.

Die MOD's bzw. Patches werden in der Regel bei der Telekom auf den Testanlagen in Nürnberg auf Zuverlässigkeit überprüft; hierfür stehen auch automatische Fernmeldeverkehrserzeugungsmaschinen (sorry, amtlichen Begriff verlegt) zur Verfügung die eine einstellbare Gesprächslast erzeugen. Dabei wird registriert, wie sich die Anlage bei welcher Last verhält. Derartiges nützt allerdings auch nichts, wenn bei der Telekom - wie bei der MOD900 von SEL - vor lauter Arbeitseifer niemand bemerkt, daß der 1. Januar ein Feiertag ist...

Die der Vorgehensweise des Herrn Haag zugrundeliegende Philosophie beruht auf der Erkenntnis, daß die praktizierte Sicherheit durch Geheimhaltung (security by obscurity) eben keine ist. Daß man Sicherheit am ehesten

dadurch erreicht, daß man alle Informationen über die Prinzipien und Arbeitsweisen offenlegt, so daß allen Beteiligten das Mitdenken über Sicherheitsverfahren ermöglicht wird.

Zumindest im Zuständigkeitsbereich von Herrn Haag hatte man durchaus den Eindruck der Transparenz über die Funktionsweise bestimmter Befehle und Systeme (siehe z.B. EWSD-Teilnehmerkonfigurations-Befehle,in dieser Datenschleuder) und organisatorischer Abläufe (siehe Kasten, ANIS-Bug und Bearbeitung durch die Telekom).

Eher spontan kam dann noch die Idee auf, das Zentrum für Kartenanwendungen der Telekom zu besuchen; ebenfalls in Nürnberg. Nach telefonischer Ankündigung bei einer leitenden Mitarbeiterin konnten auch hier Teile des Betriebs besichtigt werden, so unter anderem der Versandbereich für den Sammlermarkt.

Im Keller des Gebäudes durften wir nach mehreren dicken Stahltüren einen Blick (ohne Betreten des Raumes) auf die vollautomatische Versandanlage werfen. Die ersten Fragen, eher allgemeiner Natur, wurden noch brav beantwortet.

Als allerdings dann die ersten etwas tiefergehenden Fragen aufkamen, etwas nach der T-Card und den zugrundeliegenden Zahlenspielereien war die chinesische Mentalität einiger Mitarbeiter auf einmal wieder voll da; Studenten, die zu viele Fragen stellen, erschießt man doch eher, als daß man ihnen Antworten gibt.

Nur durch den persönlichen Einsatz von Herrn Haag konnte wohl eine Hinzuziehung der Betriebssicherung und eine damit verbundene präventive Liquidierung verhindert werden. Allerdings gelang es Herrn Haag lediglich, physische Gewalt zu verhindern, zu den gestellten Fragen wollten die Mitarbeiter - trotz guten Zuredens - zunächst einmal nichts sagen.

Der Unterschied zwischen den durch Haag gebrieften Mitarbeitern und den sonstigen Telekom-Vertretern wurde hier jedenfalls deutlich. Das Treffen hatte zur Folge, daß zunächst einmal ein Austausch von Unterlagen vereinbart wurde. Das Zentrum für Netzsicherheit bekommt einen kompletten Satz von Datenschleudern und verfügbaren CCC-Materialien im Austausch gegen Telekom-Unterlagen (Wunschliste wurde bereits überreicht, Tip: FTZ-Druckschriftenverzeichnis besorgen).

Die Unterlagen sind zwar in der Schwenckestr. 85, D-20255 Hamburg (zum Mitschreiben für die Pressestelle der Telekom) noch nicht eingetroffen, werden es aber hoffentlich bald.

Naja, und inwieweit sich die sonstigen Arbeitsweisen der Beteiligten ändern werden, wird sich zeigen. Begrüßenswert wäre natürlich, wenn in Zukunft statt einer Hausdurchsuchung mit dem beliebten Betriebssicherungs-Überfallkommando eine diplomatische Lösungsalternative bestünde. Eine telefonische Anfrage beim Beteiligten (bzw. CCC) etwa nach der Ursache der extremen Belastung eines 0130 Rufnummernkontigents könnte vielleicht zu einer geschickt distributierten Information in den entsprechenden Boards führen und nicht zu entsetzten Eltern und eingetretenen Türen.

Apropos: eine der "offen" gestellten Fragen unsererseits war natürlich die nach dem Scannen von 0130er-Nummern - ob man hier mit Par. 3 (d) der AGB (übermässige Inanspruchnahme des Telefonnetzes) in Konflikt gerät. Haags Antwort war (für seinen Bereich) deutlich; solange weder Anlagen noch Teilnehmer Unverhältnissmässig in Mitleidenschaft gezogen werden ist es kein Problem.

Blueboxing kann er übrigens nicht wirklich leiden, auch wenn das Vertrauen in die Filter nach wie vor besteht. Seine Unsympathie begründete er mit der technischen Abrechnungssystematik internationalen Fernmeldeverkehrs und ihren Auswirkungen auf das Service-0130 System aus. Den abgesehen von der Berechnung der Einheiten in der "vermittelnden" Service-0130 Anlage zwischen Ortsebene und Auslandsamt findet eine zweite Zählung dort statt.

Konkret läuft es so, dass z.B. einfach die Minuten von Deutschland nach Amerika gezählt und gezahlt werden. Die Gesprächsminuten von Amerika nach Deutschland zählt

und zahlt umgekehrt die amerikanische Seite. Diese Gesprächsminuten werden dann miteinander verrechnet; und was übrig bleibt zahlt jeweils die abgehende telefonierende Seite. Natürlich gibt es in den jeweiligen Ländern auch "Kontrollzählungen" für die ankommenden Gesprächsminuten; Phreaker sind in der Regel diejenigen, die dafür sorgen daß die beiden Zählungen nicht miteinander übereinstimmen. Alle zwar technisch abgehend aber gebührentechnisch "ankommend" geführten Gespräche (wie: R-Gespräche, Toll-Free Nummern der ausländischen Telefongesellschaft bzw. von Kunden des anderen Landes) werden manuell erfasst und über die ITU verrechnet.

Die ITU ist Koordinationsstelle für die "green numbers", damit es Kunden ohne Riesenbürokratie ermöglicht wird, toll-free nummern in allen Ländern zu bekommen die das technisch ermöglichen.

Soviel dazu. Das Netzsicherheitszentrum wurde sich natürlich wünschen, bei Fehlern im Telekom-Netz direkt informiert zu werden, anstatt davon aus der Zeitung zu erfahren. Dies hätte evtl. auch den Vorteil, daß Fehler, die im Datenschutz-Interesse aller Kunden liegen, schneller behoben werden könnten. Denn spätestens der ANIS-Bug hat gezeigt, daß ein Bericht in der Funkschau nicht dazu führt, daß der Fehler zum Telekom-Netzsicherheitszentrum (und damit zur Softwareverbesserung) durchdringt, sondern höchstens, daß er in einem anderen Arbeitsbereich der Telekom als Schädigung für den Börsengang registriert wird. Und den Börsengang der Telekom schädigen, das wollen wir doch wirklich nicht, oder?

Andy

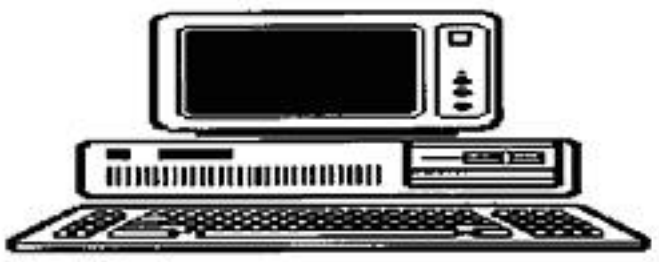
-t--- e r r o r

Für den kleinen Lauschangriff zwischendurch: Der Anis-Bug

Wie bereits in der letzten Datenschleuder erörtert, begab es sich mit der Einführung der "ANIS" -Leistungsmerkmale (Analoge Teilnehmer an ISDN-fähigen Vermittlungsstellen) daß eine Mithörmerkmal für fremde Gespräche - scheinbar aus Versehen, weil ungesteuert - implementiert wurde. Der Fehler wurde auf dem Chaos Communication Congress im Dezember 1994 (!) dem anwesenden Leiter des Privatkundenvertriebs, Klaus Busch, mitgeteilt. Die Funkschau berichtete einige Wochen nach dem Kongress über den Fehler - formell wurde er allerdings erst am 17.5.1995 (++ 4,7 Monate !!) registriert.

Im Detail sah das so aus, daß wenn ein Teilnehmer A ein Gespräch mit B führte, dann A mit Makeln auf einer "zweiten" Leitung ein C anrufen wollte - bei dem aber besetzt war - und während dieses Besetztzeichens B auflegte der A Teilnehmer auf einmal in einer fremden Leitung lauschte.

In der "amtlichen" Fehlerbeschreibung der Fehlermeldung X42868 vom 29.05.95 liest sich das so: "ANIS-TLN LM RCKFR U. MAK MITHOEREN V. VERB" - die Langversion:



"Der Fehler tritt durch die Kombination von Intercept (Verbindung zu einer Ansage) nach Talk-Zustand und dem Feature Makeln oder Dreierkonferenz auf. Mit dem Patch L3669 wird ein INTERCEPT nach dem Talk-Zustand verindert. Der eigentliche Grund zum Anlegen einer Ansage beim A-TLN nach dem Gesprächszustand kann in diesem Fall am Disconnect-Cause >Invalid-Message< der B-Seite liegen und sollte daher überprüft werden. Die Patchkorrektur L3669 wird mit dem Patchpaket N68 bei der ZSB eingereicht."

In der Praxis bedeutete dies, daß die ersten "ANIS-Bug" freien EWSD-Vermittlungsstellen hierzulande Anfang September 1995 (++ 4 Monate !!) anzutreffen waren.

Module – Gesamtübersicht

Modul 10 · Siemenschip
(P24 '90) – G&D, ODS –

geteilt, 8 Felder, Außenmaß ca. 12*12 mm

Modul 11 · Siemenschip
(P04 '91) – G&D –

geteilt, 6 Felder, Außenmaß ca. 12*8 mm

Modul 201 · Siemenschip
(P01 '91, S19 '91) – ODS, Gem* –
Modul 202 · Thomsonchip
(S64, 75 '92) – Gem* –

geschlossen, 8 Felder, Mitte achteckig, ca. 3,5 mm Durchm. Außenmaß ca. 12*10,5 mm

Modul 21 · Thomsonchip
(P18 '93, S46 '92 – Teilauflage –) – Gem* –

wie Modul 201/202, jedoch Mitte rund

Modul 22 · Thomsonchip
(P12 '92) – G&D –
Modul 22F · Thomsonchip
fluoreszierend, (S134A '93) – G&D –

wie 20, jedoch Mittelfeld kleiner, 3 mm Durchm., Goldton hell

Modul 231 · Siemenschip
(S139 '93) – Gem* –
Modul 232 · Thomsonchip
(K8S1 A/B/C 02'93) – Gem* –

wie 22, jedoch leicht geändertes Layout, Schenkelwinkel flacher, Goldton dunkel

Modul 24 · Siemenschip
(S19 '94) – Gem* –

wie 22, jedoch Ecken weniger rund, Häkchen zum Innenfeld, waagrechte Linien rötlich

Modul 30 · nicht fluor.
(S41 '92) – G&D, ODS –
Modul 30F · fluoreszierend
(S43 '92) – G&D, ODS, ORGA –

geschlossen, 6 Felder, Außenmaß ca. 11*8 mm, beide mit **Siemenschip**

Modul 31 · nicht fluor.
(P08 '94 – Teilauflage –) – G&D –
Modul 31F · fluoreszierend
(P04 '93) – G&D, ODS, UNIQA –

wie 30, jedoch geändertes Layout, Innenfeld etwas kleiner, Ecken transparent, beide mit **Siemenschip**

Modul 323 · Philipschip
(P17 '93) – Uniqa –
Modul 321 · Siemenschip – Euromodul –
(PD2 '95 04/05/06 95, A10 '96)

Außenmaße wie 30/31, mittleres Feld rechteckig ca. 3*2,5 mm

Modul 33 · nicht fluor.
(S04 '94) – ODS –
Modul 33F · fluoreszierend
(S35 '94 – Teilauflage –) – ODS –

Außenmaße wie 30/31, senkrechte Linien oben und unten abgeknickt, beide mit **Siemenschip**

Modul 34 · nicht fluor.
(P07,09 '94 – Teilauflage –) – G&D –
Modul 34F · fluoreszierend
(O2948 '94)

wie 31, jedoch Ecken schwarz, Innenfeld etwas kleiner, beide mit **Siemenschip**

Modul 35Fm · fluoreszierend
(P19 '94) – G&D –
Modul 35Fo
– m – mit, – o – ohne Schriftzug Siemens

Außenmaße wie 30/31, geändertes Layout, beide mit **Siemenschip**

Modul 40 · laminiert
Ecken eckig
(P12 '91 – Teilauflage –) – ODS –
Modul 41 · geklebt
Ecken abgerundet
(P12, P20C '91 – Teilauflage –) – ODS –

geschlossen, 6 Felder, Außenmaß ca. 12*10 mm, Mitte quadratisch 3*3 mm, beide mit **Siemenschip**

Modul 42 · Siemenschip
(P15 '91) – Solaic –

geschlossen, 8 Felder, Außenmaß ca. 12*10 mm, Mitte quadratisch 3,5*3,5 mm

Modul 431 · Siemenschip
(P05 '92) – Solaic –
Modul 432 · Thomsonchip
(S123 – Teilauflage –) – Solaic –

wie Modul 42, jedoch geändertes Layout, rechte schräge Schenkel wesentlich kürzer

Modul 441 · Siemenschip
(S101 '93 – Teilauflage –) – Solaic –
Modul 442 · Thomsonchip
(P01 '93 – Teilauflage –) – Solaic –

wie Modul 43, jedoch Innenquadrat kleiner, ca. 2,8*2,8 mm,

Modul 50 · Siemenschip
(P21 '91, S51 '92) – ODS –

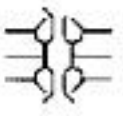
geschlossen, 8 Felder, Außenmaß ca. 13,5*11,2 mm, Mitte quadratisch 3*3 mm

Modul 511 · nicht fluor.
Siemenschip, (S57 '92) – ODS –
Modul 512 · nicht fluor.
Thomsonchip, (S129 '93 – Teilauflage –) – ODS –
Modul 51F1 · fluoreszierend
Siemenschip, (S51 '92 – Teilauflage –) – ODS –
Modul 51F2 · fluoreszierend
Thomsonchip, (S02 '94 – Teilauflage –) – ODS –

wie 50, jedoch Mittelfeld kleiner, ca. 2,8*2,8 mm

Modul 60 · silbern
Thomsonchip, (P05 '93) – Schlumberger –

geschlossen, 9 Felder, Außenmaß ca. 13*10,5 mm



Modul 61 · silbern
Siemenschip, (P21 '94) – Solaic –

geschlossen, 8 Felder, Außenmaß ca. 11*10 mm

Stand: 06.09.1995

Zentrum für Kartenanwendungen der Telekom,
Postfach 443322, 90206 Nürnberg

Tel: EWSD-DIV ASP

(...auszug anschlussprotokoll...)

```
(Standard-DIV "ANIS"-Anschluss)
01K4S/9124  K4S  D/DBPXBZ0V1032-E25/010          96-02-31     23:42:28
3781          OMT-00/SCHNEIDE       2816/03800

PROTTLN:ONKZ=09124,RN=4088

OKNZ =09124 RN = 4088 LAG = 100- 0- 0- 2
        ATYP     =AAS
        ANZVERB =1
        ARU      =ARUBES    ARUBSAEN ARUZEIT ARUZTAEN ARUSOF
                  ARUAEND   DDVBY    DDVDA   DDVIN
        LATT     =TAWA      GBZI
        GEB      =EGN
        DAT      =AKTAKL    FANE     KONF3   KONFG    WAFAKT
                  FANHALT1  RRB
```

(DSS1)

```
01K4S/9124  K4S  D/DBPXBZ0V1032-E25/010          96-02-31     23:42:28
3781          OMT-00/SCHNEIDE       2816/03800

PROTTLN:ONKZ=09124,RN=4640

ONKZ = 09124     RN=4640          LAG    = 90- 1- 2- 1

        ATYP     =IBA
        ANZBKAN =2
        LATT     =MRN        ALLNR
        GEB      =EGN
        DAT      =GEAUFVER  MRNSTD
        ZUSINF   =MULTILAG
      DIENST   =LDSPRACH
        ARU      =ARUBES    ARUBSAEN ARUZEIT  ARUZTAEN ARUSOF
                  ARUAEND   DACTDVBY DDVBYCF  DDVBYFN  DDVBYN
                  DACTDVDA DDVDACF  DDVDAFN  DDVDAN   DACTDVI
                  DDVICF    DDVIFN   DDVIN    ARURZ    DDVCDEFN
                  DDVCDEN
        SUBADR   =SADTRANS
        GEB      =GEBANZLF
        DAT      =AKTAKL    RCKFRAGE KONF3    ARNA     UMSTBUS
                  AZASIG    BRNA     AKLMRTLN
```

ONKZ	Ortsnetzkennzahl
RN	Teilnehmerrufnummer
GEB	Gebuehrenverfahren
LSCHGEB	Werte fuer Gebuehren loeschen
LATT	Leitungsattribute
ALLNR	Alle Nummern
GBZI	Gebuehrenzaehlimpulse
MRN	Mehrfach-Rufnummer
RUFUNT	Rufunterscheidung
ZUSTABFR	Zustandsabfrage moeglich
LSCHLAT	Werte fuer LATT loeschen
SPER	verwaltungsbedingte Sperre
LSCHSPE	Werte fuer SPER loeschen
DAT	Anschlussdaten:
ADMRCKS	Ber., Allg. Dienstmerk. Ruecks.
AKTAKL	Anklopfen aktiviert
AKTGDS	Gespraechsdatenschutz aktiviert
ARNA	A-Rn bei B-Tln angezeigt
ARNN	A-Rn bei B-Tln nicht angezeigt
ARNNAKT	Ber. zur arnn-aktivierung
ARNNIGN	ARNN wird ignoriert (!)
ARW	Anrufweiterschaltung
ARWA	Anrufweiterschaltung durch A-tln
B1RNA	B1-Rn wird bei B-Tln angezeigt
B1RNN	B1-rn wird bei b-tln n. angezeigt
B1RNNAKT	Ber. zur B1RNN-aktivierung
AR1NNIGN	B1RNN wird ignoriert
DSCH	Schutz wichtiger Dienste
FKATAST	Fernkatastrophenberechtigung
GDSAKT	Ber.,gespr.Datenschutz z.akt
GEAUFVER	generelle Aufschaltverhinderung(!!)
NLISTRN	Rufnummer nicht aufgelistet
RRB	Rueckruf bei belegtem Teilnehmer
WAFAKT	Berecht.z.Áktivieren v.Anklopfen
FANE	Fangen mit einleiten
FANS	Fangen sofort
FANHALT1	Fangen mit halten absolut
KONF3	Dreierkonferenz
RCKFR	Rueckfr. moeglich
ARNAANF	ARNA auf Anforderung
ARNNANF	ARNN auf Anforderung
ERKZ1	erhoehte Rufkennzahl 1
ERKZ2	" 2
ERKZ3	" 3
RRBWTS0	Rueckruf bei bel. Tln., wart.schl.0
RRBWTS1	" 1
RRBWTS2	" 2
RRBWTS3	" 3
RRBWTS4	" 4
RRBWTS5	" 5

LSCHDAT	Werte fuer DAT löschen
UK1	Ursprungskennung 1
UK2	" 2
DATNR	Anschlussdaten mit Nr.
LDATNR	Werte f.DATNR löschen
VOWAEN	Berechtigung, Verb ohne Wahl zu Ändern
VOWSOF	Verb. ohne Wahl sofort
VOWVER	Verzögerte Verb.o.Wahl
SABBD 10	Shrd.abb.dial.shortno.
10T	Berechtigung zur Ver-
100	wengung der zweistel-
20	ligen Kurzwahlliste
30	(kw xx) eines anderen
90	Teilnehmers
VEREIN	Verkehrseinschränkugen
LVEREIN	Werte f.VEREIN löschen
VERKLBED	Werk.einschr.kl.d. Bediener eingaben
LVERKBED	Werte f.VERKLBED löschen
VERKLTLN	Verk.einschr.kl. d. Tln.anford.
LVERKTLN	Werte f. VERKLTLN löschen
LTT	Ltg-Übertragungstyp
ARU	Anrufumlenkung
LSCHARU	Werte fuer ARU löschen
KW	Kurzwahldaten
LSCHKW	Werte f. KW löschen
KWUN	Kurzwahl uneingeschr.
LSCHKWUN	Werte f. KWUN löschen
ANZVERB	Anzahl d. erlaubten Verbind.

0010101010010101100110101001010110
1010101000101010100101010101010010
101001010100101abgetipptvonf.10101
0100101010101101010101010101101010
1010101010001001001010101101010001
0010010011010110101101011010110101
1010110101101011010110101101011010
1101011010110101101011010110101101

Kryptisches...

To: cypherpunks@toad.com
From: Matt Blaze <mab@research.att.com>
July 18, 1996

There is currently being circulated, to members of Congress and possibly elsewhere, a four page document entitled ``Brute-Force Cryptanalytic Attacks'' that calls into question some of the conclusions of the ``Minimum Key Lengths for Symmetric Ciphers'' white paper [1]. The document bears no author or organization attribution, but we are told that it originated from NSA.

The NSA document argues that ``physical realities'' make parallel key search much more expensive and time consuming than our white paper estimated. However, the NSA document appears to have been written from the perspective of general parallel processing or cryptanalysis rather than exhaustive key search per se. It ignores several elementary principles of parallel processing that apply specifically to exhaustive key search machines of the type that our white paper considered.

In particular, NSA argues that interconnections, heat dissipation, input/output bandwidth, and interprocessor communication make it difficult to ``scale up'' a key search machine by dividing the task among a large number of small components. While these factors do limit the scalability of more general purpose multiprocessor computers (such as those made by Cray), they do not apply at all to specialized exhaustive key search machines. The NSA argument ignores the most fundamental feature of brute-force key search: the processors performing the search have no need to communicate with other components of the system while they perform their share of the search, and therefore the system has no need for any of the global interconnections that limit scaling. Indeed, there is no reason that all the components of a parallel search machine must be located even within the same city, let alone the same computer housing. We note that one of our co-authors (Eric Thompson, of Access Data, Inc.) designs and builds medium-scale FPGA-based key search machines with exactly this loosely-coupled structure, and regularly uses them to recover keys for clients that include the FBI.
The NSA document also calls into question our cost estimates for ASIC components, suggesting that ASIC chips of this type cost NSA approximately $1000.00 each. However, our $10.00 per chip estimate is based on an actual price quote from a commercial chip fabrication vendor for a moderate-size order for an exhaustive search ASIC designed in 1993 by Michael Wiener [2]. Perhaps NSA could reduce its own costs by changing vendors.

Finally, the NSA report offers estimates of the time required to perform exhaustive search using a Cray model T3D supercomputer. This is a curious choice, for as our report notes, general-purpose supercomputers of this type make poor (and uneconomical) key search engines. However, even the artificially low performance results for this machine should give little comfort to the users of 56 bit keys.
According to NSA, 56 bit keys can be searched on such a machine in less than 453 days. ``Moore's law'' predicts that it will not be long before relatively inexpensive general-purpose computers offer similar computational capability.

/s/ Matt Blaze
Whitfield Diffie

References:

[1] Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. ``Minimum Key Lengths for Symmetric Key Ciphers for Commercial Security.'' January 1996. Available from ftp://ftp.research.att.com/dist/mab/keylength.txt

[2] Wiener, M. ``Exhaustive DES Key Search.'' Presented at Crypto-93, Santa Barbara, CA. August 1993. s lion.

Ausland

More about the bust about the Argentinian hacker, Ardita

Ok, to clarify a bit whats going on with this 'Argentinian that broke into this and that' Julio Ardita, known as 'El Griton' (The Screamer) has been around for about 4-5 years now, back then his main motivation was to get on QSD (A french X.25 chat system) and trade PADS and codes and that kind of shit, as well as chat with the people in there. At that moment I can positively say he was completly clueless.

Some time after that he formed, a haq group (or warez, didnt really know) called 'White Lands' pretty much clueless too. He ran a board called 'Scream' which is English for 'grito', he put out some t-files, cut and pasted text from online manuals of ARPAC (the Argentinian x.25 net, now called STARNET)

I never talked to the guy voice, at the time i met him (4 years ago at a friends party) he couldnt tell a computer from a microwave oven, yet he considered himself a haqr, anyway, thats the only time i saw him personally. We all started as clueless as it could be and eventually learned lots of stuff...

What he did:
He had been using an account at husc8.harvard.edu for quite a long time, many others shared that account, dunno if it was posted on some BBS, passed over or what. From there all sort of shit was done by lots of haqr types. He and the others blueboxed that way to harvard's dialups, eventually BB in .ar cameto an end ond the vast majority of bboxers quit doing it.

He obtained accounts on a coupple of local systems, where he logged to dialing in from his home, one of this systems is an university located in another city (ld call).

Then, someone posted the 0-800 (== 1-800) dialup to Telecom's (one of the 2 telcos in Argentina) PSDN, an x.25 net called Telconet on several BBSes. Telconet uses the good 'ole Telenets soft, yes, yes with 'pad-to-pad capabilities', it links a net of mostly AIX RS/6000 boxes, running TCP/IP over x.25 and over 2.048Mbs in certain areas, access to these boxes from the dialup is pre-validated by TAMS...for MOST OF THE NUAS BUT NOT ALL OF THEM, he broke into a rs6k box that did not required TAMS validation, he used a passwordless account...

From there he tried to break into (or actually did) several internet hosts, as this particular AIX box on Telconet had inet connectivity, he telneted to his other had accounts in .ar and other countries, he tried to break in to <sumhost>.navy.mil , i dunno if he acomplished this, but obviously someone at the .mil site noticed and sent mail to root at the telco host or noc/nic, mail went back and forth, to cert , to all the other places he connected to, etc.

Telco personel didnt have to do much to get the guys phone number, since he was calling from his home to a 0-800 owned by the telco and ANIed up its ass and all over the rest too.

Dec 30, 1995, El Griton got busted, his computer seized, all the usual stuff, Telecom also had recordings of his voice calls, the FBI was also involved in this (due to the .mil part i suspect). This was the front page of the newspapers for 2 days... yeah, this part as usual too, incredible bullshit mixedwith hidden lobby for passing certain laws and a bit of gasoline to the fire of the quiet fight between the telcos and the multimedia emporiums, cable-tc+open-air-tv+newspapers corporations.[This all, is of course my personal view of the facts]

So from then on things dissapeared from the media, nothing else was know until today...

Stuff found on his accounts:
irc executable
coupple of 8lgm's exploits
ISS output
etc.

PS: CERTs reference number for this incident is CERT#11802
Opii (of HBO)

Chaos Computer Club e.V.
Schwenckestr. 85

D-20255 Hamburg

Hamburg, den 03.05.96

P[redacted]
P[redacted]
STA. [redacted] - PF [redacted]

D - [redacted]

Sehr geehrter Abonnent,

bei einem Blick in unsere Datenbank stelten wir fest, dasz Ihr Abonnement mit der Nummer 47 ausgelaufen ist.

Um dieses zu verlaengern ueberweisen Sie uns bitte

Abonnement (normal) = 60.- / 8 Ausgaben,

Auf unser Konto:

Chaos Computer Club e.V. (Kto-Nr.: 0599090-201) bei der Postbank Hamburg (200 100 20).

Mit freundlichen Gruessen
Chaos Computer Club e.V.

YS

Abl. n 7.w.V.

7.5.96

EINGEGANGEN 1 3. Juni 1996

Staatsanwaltschaft [redacted]

Staatsanwaltschaft [redacted] Postfach [redacted]

Chaos Computer Club e.V.
Schwenckestr. 85

20 255 Hamburg

Postfach [redacted]
[redacted]
Telefon [redacted]
Durchwahl:
[redacted]
Telefax: [redacted]

Datum: 24.05.1996

Aktenzeichen:
[redacted]
(Bitte bei allen Schreiben angeben)

Sehr geehrte Damen und Herren,

ohne nähere Hinweise oder Angabe des hiesigen Aktenzeichens kann Ihre Eingabe vom 03.05.1996 nicht untergebracht und das angeblich bei der Staatsanwaltschaft [redacted] laufende Strafverfahren nicht ermittelt werden.

Ebenso ist ein Abonnement unsererseits bei Ihnen nicht bekannt.

Hochachtungsvoll

[redacted]

Oberstaatsanwalt

Beglaubigt

[redacted]

Justizangestellte

Das Jahr 00

Die Daten und die Daten

Ungefähr 42 (!) Monate trennen uns noch vom "heiligen Jahr", dem 2000ten Jahrestag dessen, daß "ein Mann an einen Baumstamm genagelt wurde, weil er gesagt hatte, wie phantastisch es doch wäre, wenn die Leute zur Abwechslung mal nett zu einander wären".

Die Chancen stehen ganz gut, daß aus diesem Anlaß mal wieder ein paar Leute an Baumstämme genagelt werden, oder zumindest anderweitigen physischen Schaden nehmen. Dies dürfte nämlich die unweigerliche Folge davon sein, daß es für einige tausend Softwareprojekte auf diesem Planeten eine Deadline gibt, die nicht von irgend einem Vertriebsheinz oder Marketingfuzzi festgelegt wurde, sondern von den fernen Vorgängern der jetzigen Akkordprogrammierer unausweichlich und letztgültig festgecoded wurde.

Die Rede ist vom Jahr-2000-Problem, auch wunderschön neuenglisch "the millenium bug" genannt. Da niemand in der schnellebigen Softwarewelt an das übermorgen denkt und es sich mit kleinen Variablen sowieso viel schöner programmieren läßt, ist ein ziemlich großer Teil der Software, die noch auf den Groß- und Kleinrechnern der Welt nur mit einer zweistelligen Repräsentation für die Jahreszahl ausgestattet. Den Spaß, zu dem das führt, wenn die auf Jahreszahl auf 00 sprigt, haben heute schon die Leute, die über 100 Jahre alt sind. Die bekommen dann Musterungsbescheide, Kindergeld, Kontokündigungen etc. Was bei Bankrechnern passiert, die plötzlich Zinsen für negative Jahreszahlen berechnen sollen, ist nicht so ganz klar. (jetziges Datum minus Einzahlungsdatum= Anzahl der zu verzinsenden Tage, 00 - 92 = -92 oder +92, wenn vorzeichenlose Integer verwendet wurden)

Selbst wenn es allen Banken gelingen sollte, ihre Software rechtzeitig umzustellen oder ihre assemblerprogrammierten BS2000-Schrankwände auf den Schrott zu fahren, bleibt noch das Problem mit den Kunden. Wenn die zur Überzeugung gelangen, daß da doch noch ein Risiko besteht, gibt es im Dezember 1999 ein kleines Problem mit dem Bargeldnachschub. Die wirklichen Zocker lassen natürlich noch was auf ihrem Konto, es könnte sich ja auch ein deutlich höherer Betrag einfinden. Die Information, welche Bank welchen Compiler verwendet hat, wird sozusagen bares Geld wert.

Vorbeugen könnten die Banken nur, wenn sie ihren Kunden Einblick in ihre EDV geben würden, damit die sich selbst von der Qualität der eingesetzten Software überzeugen. Dies würde allerdings eine vollständig neue Dimension im vielbeschworenen Vertrauensverhältnis Bank-Kunde bedeuten.

Letzenendes handelt sich dabei nur um die logische Weiterführung des Datenschutzgedankens. Die Forderung nach einem solchen Einblick wird im Zweifel von allen derartigen Institutionen brüsk zurückgeweisen. Schließlich könnten sich ja dabei auch Einblicke in die (obskuren) Sicherheitsmechanismen ergeben und das Vertrauen endgültig entsorgt werden.

frank@ccc.de

(Netz-) Agenten

Vertrauen ist gut, Kontrolle ist besser

In der Datenwelt tummelt sich eine Vielzahl von Computerprogrammen, die weitgehend autonom eine bestimmte Aufgabe ausführen und dabei im Auftrag einer einzelnen Nutzerin oder einer Organisation tätig sind. Software-Agenten, Roboter, Bots, Web-Crawler und Spider sind maschinelle Kreationen, die als Suchmaschine im WWW und in den News bei der Informationssuche helfen, mit denen man als Weizenbaum-Tochter ELIZA oder in MUDs und im IRC nett plaudern kann oder die als "lernfähiger" persönlicher Agent das Postfach sortieren, auf interessante Angebote hinweisen und mit anderen Agenten Termine für ihre Agentenführer ausmachen.

Viele Fragen bleiben noch offen. Wie weit können und sollen die Handlungsfähigkeiten elektronischer Agenten als Stellvertreter, Assistent oder Gegenspieler menschlicher Nutzer reichen? Welche Aspekte der Gestaltung des Netzverkehrs können und sollen an Agenten delegiert werden? Wer entscheidet darüber, wofür und wo Agenten eingesetzt werden? Wie läßt sich erreichen, daß die Beanspruchung von Netzressourcen, die mit dem Auftreten von immer mehr Bots, Agents und Spiders verbunden ist, möglichst gering bleibt? An welche Regeln sollten sich die Konstrukteure von Robotern halten? Was müßte eine Netiquette für Software-Agenten beinhalten, die sie zu guten Net Citizens macht? Wie sollten sich Agenten in der Interaktion mit menschlichen Nutzern verhalten ("Talk to my agent") und wie in der Interaktion mit anderen Agenten

("My agent talks to your agent")? Wer ist verantwortlich für die Aktionen und Transaktionen von Agenten? Wem gehören die personenbezogenen Daten, die die Agenten sammeln, und wer darf diese Daten für welche Zwecke verwenden? Sind diese Kreaturen "mostly harmless", oder ist letztlich nur den selbstgemachten Agenten zu trauen?

Die Netzgemeinde hat in den letzten Jahren eine Reihe von Lösungsvorschlägen für einige dieser Fragen entwickelt. Diese Vorschläge zielen in der Regel auf Anleitungen

für die Konstruktion von Software-Agenten und adressieren ihre Entwickler. So gibt es inzwischen einen "guide for robot-writers", der die Netzbelastung durch falsche oder ungeschickte Programmierung vermeiden helfen möchte. In Anlehnung an Isaac Asimovs Robotergesetze wurden "laws of softbotics" entworfen. Ethische Leitlinien für das Auftreten und Verhalten von Agenten wurden entwickelt.

Auf der Seite derjenigen, die von dem Treiben von Software-Agenten betroffen sind, gibt es eher noch wenige Einflußmöglichkeiten. Die Suchmaschinen für die WWW-Navigationshilfedatenbanken können bei schlechter Programmierung den Betrieb der von ihnen durchforsteten WWW-Sites empfindlich beeinträchtigen. Ihr Besuch kommt unangemeldet, und die gesammelten Informationen werden ungefragt in der heimatlichen Datenbank der Suchmaschine gespeichert. Ein Robot Exclusion Standard erlaubt es beispielsweise WWW-Anbietern umherschweifenden Spidern den Besuch ihrer Seiten zu verbieten.

Je mehr Aufgaben an Agenten delegiert werden, welche diese dann eigenständig durchführen, desto mehr besteht das Risiko, daß aus dienstbaren Nützlingen unangenehme Schädlinge werden. Die vermeintlichen Heinzelmännchen können durch zu großes Datenaufkommen den allgemeinen Netzverkehr empfindlich stören, wie es etwa bei sich unkontrolliert 'virenartig' vermehrenden Programmen vorkommt. Sie können entweder gewollt oder unbeabsichtig andere Nutzer belästigen, in dem sie z.B. private Postfächer unaufgefordert mit Werbung oder Hetzschriften vollstopfen.

Ein schlecht programmierter autonomer persönlicher Agent löscht oder unterschlägt aus "Unwissenheit" wichtige Informationen. Solches Fehlverhalten kann durch verbesserte Programmierung ausgeschlossen werden; eine andere Art von Fehlverhalten kann jedoch ein-

programmiert sein: Software-Agenten können ihren offiziellen Auftraggebern schlechte Dienste erweisen, in dem sie inoffiziell noch anderen Auftraggebern zuarbeiten. Als potentielle Interessenten für Doppelagenten wären etwa Markt- und Meinungsforscher, Firmen, Glaubensgemeinschaften, Regierungen und deren Geheimdienste oder Steuerfahndungen denkbar.

Datenbanksuchmaschinen des WWW könnten beispielsweise aus der unübersehbaren Fülle des WWW bestimmte Informationen herauswählen oder unterschlagen,ohne daß dies den Nutzern sofort auffallen würde. Irgendwann könnte man Verdacht schöpfen, wenn z.B. immer wieder dieselben Firmenangebote genannt werden oder zu einem brisanten Thema plötzlich keine WWW-Hinweise mehr ausgegeben würden. Oder man stelle sich ein arglos erworbenes Softwarepäckchen vor, das die lästige Arbeit des Netzanschlusses übernehmen soll und das aber gleichzeitig unaufgefordert Informationen über Inhalte der Benutzerfestplatte an Dritte ins Netz gibt.

Die freiwillige Selbstkontrolle und der Appell an die Eigenverantwortung vonEntwicklern und Besitzern bzw. Anwendern von Software-Agenten reichen in Zeiten, die auch in der Netzwelt rauher werden, wahrscheinlich nicht aus. Sinnvoll könnte es daher sein, eine unabhängige Prüfinstanz etwa nach dem Vorbild der Stiftung Warentest einzurichten. Diese Institution könnte als Anwalt der Netznutzer- das Gebaren von Software-Agenten stichprobenartig kontrollieren. Die Ergebnisse der Prüftätigkeit sollten im Netz verbreitet werden.

Eine Hürde für Prüfinstanzen nichtstaatlicher oder auch staatlicher Herkunft liegt darin, daß nur von solchen Softwareprodukten der Tätigkeitsbereich vollständig durchschaubar ist, bei denen neben dem Binärcode auch der Quellcode für Prüfzwecke zur Verfügung steht. Bei kommerziellen Softwareprodukten wird der Quellcode von den Herstellern zurückbehalten, denn wenn sie die Baupläne bzw. Rezepturen für ihr Produkt herausgeben würden, könnten Konkurrenten oder Kunden ihr Produkt leicht nachbauen. In der pharmazeutischen Industrie muß vor staatlichen Kontrollbehörden die Unschädlichkeit einer offenzulegenden Rezeptur nachgewiesen werden. Vergleichbares für den Bereich Software anzustreben wäre in Anbetracht der nichtvorhandenen Einflüsse auf Leib und Leben natürlich völlig übertrieben und praktisch wegen der Internationalisierung des Softwaremarktes nicht durchführbar.

Selbst wenn Übereinstimmung herrschte, daß als eindeutiges Prüfkriterium gelten soll " Ein Software-Agent hat nicht mehr als das zu auszuführen, was er auszuführen verspricht", müßten die Nutzer bei solch einer zentralisierten staatlichen oder nicht-staatlichen Lösung sich auf diese Zentralinstanz verlassen. Internettypisch und bewährt sind dagegen dezentrale Problemlösungen, die im Falle von Softwarekontrolle darin bestehen können, daß auf freie Software mit veröffentlichten Quellprogrammen zurückgegriffen wird.

Die Software-Agenten sind unter uns, und es werden immer mehr. Sie können die Handlungsfähigkeiten menschlicher Nutzer ebenso unterstützen und erweitern, wie auch einschränken. Ihr Risikopotential ist beträchtlich.

Die Koexistenz menschlicher und nichtmenschlicher Akteure in der Netzwelt und die damit verbundenen grundlegenden Fragen nach den Bedingungen der Teilhabe der maschinellen Kreaturen bilden eine netzpolitische Leerstelle. Eine breitere,

netz-öffentliche Diskussion bleibt zu wünschen.

Sabine Helmers & Ute Hoffmann

s@duplox.wz-berlin.de, uteh@medea.wz-berlin.de

Agenten: Quellen

Web-Server:
MobilAgenten Projekt Uni Stuttgart:
http://www.informatik.uni-stuttgart.de/ipvr/vs/projekte/mole.html
Diplom-Arbeit von Fritz Hohl:
http://www.informatik.uni-stuttgart.de/cgi-bin/ncstrl_rep_view.pl?/inf/ftp/pub/library/ncstrl.ustuttgart_fi/DIP-1267/DIP-1267.bib
DAFID-Seite (Links zur Mobile-Agentenforschung in Deutschland):
http://www.informatik.th-darmstadt.de/~fuenf/work/agenten/agenten.html
Metaseite (nicht nur mobile Agenten):
http://www.cs.umbc.edu/agents/

Bücher:
Agents unleashed (populärwissenschaftlich)
http://www.access.digex.net/~pcw/agunlsh.html
Internet Agents, Bots, Wanderers and Worms

Systeme:
Telescript (General Magic):
http://www.genmagic.com/
kann alles, Smalltalk-ähnliche, eigene Programmiersprache, Entwicklungstool verfügbar, allerdings unglaublich Ressourcenintensiv: - mind. 64 MB RAM für Development Kit. Wahrscheinlich nicht für offene Systeme einsetzbar. Urvater aller Mobilen-Agenten-Systeme.
Mole: http://www.informatik.uni-stuttgart.de/ipvr/vs/projekte/mole.html
demnächst verfügbar
Tacoma: http://www.cs.uit.no/DOS/Tacoma/index.html
kann wenig, macht Tcl und noch irgendwas, verfügbar
Ara: http://www.uni-kl.de/AG-Nehmer/Ara/ara_D.html
kann mehr (Tcl, C), noch nicht verfügbar
FTP Software CyberAgents *(neue Version, die alte hat damit nix zu tun :-):*
http://www.ftp.com/cyberagents/
nur für geschlossene Anwendungen, Java, ein Produkt, verfügbar
Java-to-go:
http://ptolemy.eecs.berkeley.edu/~wli/group/java2go/java-to-go.html
nur für geschlossene Anwendungen, Java, Alpha-Stadium, frei, verfügbar
<Namenloses etwas aus Frankfurt>
http://www.tm.informatik.uni-frankfurt.de/~lingnau/
baut auf HTTP auf, keine Erfahrungen, noch nicht verfügbar
AgentTcl
http://www.cs.dartmouth.edu/~rgray/transportable.html
sieht gut aus, benutzt Tcl als Sprache, verfügbar

Papers:
General Magic Whitepapers (von Jim White :-): *gibts allerdings nur in Papierform*
Are Mobile Agents a Good Idea?
http://www.research.ibm.com/massdist/
IBM Papier, relevant
Itinerant Agents for Mobile Computing:
http://www.research.ibm.com/massdist/
IBM Papier, relevant

Sonstiges:
OSF-Forschergruppe "Distributed and Mobile Objects":
http://www.osf.org/RI/DMO/DMO.htm
Joint W3C/OMG Workshop on Distributed Objects and Mobile Code:
http://www.w3.org/pub/WWW/OOP/9606_Workshop/

kleingehacktes...

From: thegnome@fastlane.net
(Simple Nomad)
Newsgroups: comp.os.netware.security
Subject: Re: ABENDING Server
Date: 16 Jul 1996 06:58:00 GMT
Organization: Nomad Mobile Research Centre

>>All,
>>Does anyone know of an easy way to
>>ABEND a **netware 3.12** server?
>>All help is greatly appreciated!

>From Simple Nomads FAQ

> Netware 4.1 : type 512 chars on the
> console + NENTER -> abend
> Netware 3.11 : NCP request 0x17-subfn
> 0xeb with a connection number
> higher than the maximum allowed will
> crash the server (yes you will
> need the APIs)

> From the next version of the faq (out in a
> couple of weeks)

- At the server console type
  UNLOAD RENDIRFX
- Use your local copy of
  SYS:PUBLIC/RENDIR.EXE
- In SYS:LOGIN type RENDIR <alt 174>
<alt 174> (login not required, just
attaching to the server)

http://www.fastlane.net/
homepages/thegnome

elektropost...

From 100542.1571@CompuServe.COM
Wed Jun 12 18:07:35 1996
Subject: Frage nach "Worlds Within" BETA Testern

Liebe Freunde und Freundinnen,

in wenigen Stunden launchen wir unsere Serverside und die Clients, die Clients distributieren wir entweder per Diskette oder zum downloaden. Es würde uns sehr helfen und freuen wenn ihr euren Freundeskreis informieren könntet damit wir Interessierten die Downloadadresse bzw. die Disketten zusenden können.In den exclusiven Kreis der Betatester können alle eintreten, die gewillt sind auch Feedback auf "Worlds Within" zu geben.

Die Hardware - Anforderungen fuer einen Betatest side sind:

486 DX 66 bis Pentium PC 200 HZ - mindestens 8MB RAM, besser 16 MB - WINDOWS 95 als System - Modem ISDN oder 14400 bis - Prowider der Telnet und FTP ermoeglicht - Anmeldungen entweder ueber diese E-mail Adresse oder ueber Fax ++49-40 76910544.

ACHTUNG!! Die erste Betaversion "Worlds Within" beinhaltet nur 2 Tools: Navigation und Chat.

Wir planen Schrittweise Updates in den nächsten Wochen

Vielen dank mit grüßen Van Gogh TV

Techno-Terrorismus?

Riegersches Weltuntergangstheorem

London, irgendwann Mitte der 90er Jahre.

Ein gediegenes Haus im Finanzdistrikt, eine sogenannte erste Adresse. Vier Männer in perfekt sitzenden Maßanzügen betreten die Räume einer großen Investmentbank. Bei sich führen sie zwei mittelgroße, offenbar schwere Reisekoffer.

Sie begeben sich direkt in das Büro des Direktors, sie werden dringlich erwartet. Im schall-isolierten Besprechungsraum begrüßen sie drei Herren mittleren Alters, alle mit der typische Ausstrahlung machtgewohnter Senior Manager, die alle einen sichtbar schlechten Nachtschlaf hatten.

Vor der Tür stehen zwei professionelle Sicherheit verkörpernde jüngere Männer mit militärisch kurzem Haarschnitt und etwas auftragenden Jacken. Drinnen werden die beiden Koffer mit zwei dicken Kupferseilen verbunden, einer aus der Vierergruppe erkundigt sich fürsorglich, ob etwa ein Herzschrittmacherträger in der Nähe sei. Daraufhin verläßt einer der Manager fluchtartig den Raum und sucht eilig das Weite.

Eine kurze, merkwürdig aussehende Antenne wird an einen der Koffer angeschlossen und auf einige an der Aussenwand stehende, in betrieb befindliche Computer gerichtet. Die Anwesenden treten ein paar Schritte zurück, ein tiefes Brummen gefolgt von einem kurzen aber scharfen elektrischen Knistern erfüllt den Raum. Die Rechner in der Ecke haben als letzte Lebenszeichen eine kleine Rauchwolke abgesondert. Nicht einer läßt sich wieder in Betrieb nehmen. Einer der Koffererträger bittet die Manager ans Fenster und zeigt ihnen einen LKW, der einen Block weiter parkt.

Danach überreicht er eine kleine Karte, die in edlen Lettern die Koordinaten eines Kontos in der Schweiz, eine Zahl mit relativ vielen Nullen am Ende und die lakonische Zeile "Vier Stunden. Keine Nachforschungen." aufweist. Die Herren verabschieden sich freundlich, aber kurz und verlassen das Haus.

Dreieinhalb Stunden später werden 10 Millionen Pfund von einem niemals zuvor oder danach benutzen Züricher Konto in mehreren tausend kleinen, unter der Auslöseschwelle der Anti-Geldwäsche-Systeme liegenden Transaktionen rings um die Welt verteilt.

So oder so ähnlich sollen sich über 40 Fälle von Erpressung zugetragen haben, wenn man den Recherchen eines britschen Journalisten der Sunday Times glauben möchte. Der angebliche Gesamtschaden soll etwa eine Milliarde Mark betragen.

Die Bewertung der Glaubwürdigkeit dieser Geschichte gestaltet sich aus verschiedenen Gründen problematisch. Die betroffenen Unternehmen (vor allem Banken aber auch Rüstungsunternehmen) haben naturgemäß keinerlei Interesse an einer öffentlichen Erörterung solcher Probleme.

Die Aussage, daß Kampfmittel aus dem Bereich der sogenannten Information Warfare (nichtnuklearer EMP, HERF/HIRF) gegen zivile Organisationen angewand wurden, läßt sich nach dem gegenwärtigen Stand der Informationen nicht wirklich verifizieren.

Nach den Erfahrungen, die der CCC im Rahmen der Aufklärung einer kleineren Sicherheitsschwankung gemacht hat, ist im Zweifel auch gar kein Einsatz von derartigen Mitteln erforderlich, um Banken u.ä. zu erpressen. Alleine die Vorspiegelung von genügender technischer Kompetenz, die es als möglich erscheinen läßt, das der Erpresser über die entsprechenden Fähigkeiten verfügt, führt in den allermeisten Fällen zur Zahlung der geforderten Summe.

Dank der unermüdlichen Tätigkeit von telegenen Fönfrisurenträgern wie dem amerikanischen "Sicherheitsberater" Winn Schwartau - der, nicht ganz zu Unrecht auch schon als Computerapokalyptiker tituliert

wurde - hat sich in den entsprechenden Kreisen eine solide Furcht vor Angriffen auf die EDV breitgemacht. Die ökonomisch Verantwortlichen haben oft ein eher irrationales Verhältnis zu Computern.

Das wirkliche Ausmaß der Abhängigkeiten von rechnergestützten Systemen und Netzwerken ist den meisten Verantwortungsträgern nicht bewußt und teilweise wegen gerontologischer Hinderungsgründe auch nicht beizubringen. Insofern ist eine reale Abschätzung der Bedrohungslage für sehr viele Manager nicht möglich. Offenbar gilt bei nahezu allen Unternehmen, egal ob Banken, Rüstungskonzerne oder chemische Industrie, der Grundsatz, daß bei ausreichend glaubwürdiger Bedrohung gezahlt wird.

Das Risiko, daß bei Ermittlungen Informationslecks entstehen und es womöglich zu einem öffentlichen Interesse an dem Fall kommt, wird geradezu paranoid gefürchtet. Den damit wird die Funktionsweise einer Bank vom Prinzip her gefährdet; die Deutsche Bank formuliert es in Anzeigen mit dem Satz "Vertrauen ist der Anfang von allem."

Im Falle der erwähnten Sicherheitsschwankung war ein Mann namens Ungerbühler, der aus einer psychatrischen Klinik ausgebrochen war, an verschiedene Unternehmen mit Geldforderungen herangetreten.

Er behauptete Mitglied des CCC zu sein und durch Hacking etc. an unternehmensinterne Daten über Steuerhinterziehungen etc. gekommen zu sein. Unter Vorlage seines echten Ausweises kassierte er mehrfach und regelmäßig mehrere tausend Mark, wobei er gelegentlich Disketten mit "Daten" übergab.

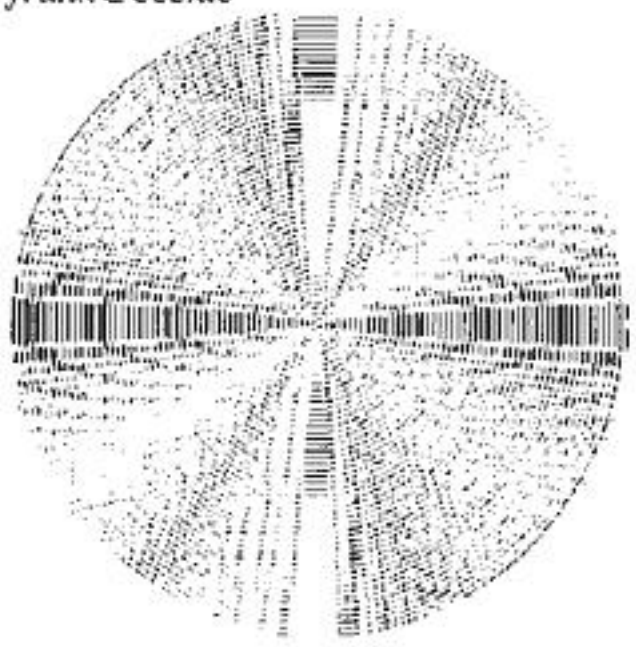
Wie die panischen Sicherheitsbeauftragten der erpressten Konzerne regelmäßig feststellten, hatten sie einige sehr teure Leerdisketten erworben. Unter den genarrten Firmen waren Großbanken, Rüstungsunternehmen aber auch Mittelständler. Die Ziele für seine Aktionen wählte Markus Ungerbühler teilweise nach Presseberichten über Firmen aus, die z.B. Probleme mit dem Finanzamt haben. Ungerbühler wurde, nachdem er seine "Geschäfte" über Monate hinweg unbehelligt betreiben konnte, nicht zuletzt durch die Aktivitäten von privaten Sicherheitsorganisationen, die im Auftrag von betroffenen Firmen arbeiteten, festgenommen und in seine Klinik zurückgebracht.

Stellt man die Erkenntnisse aus dem Fall Ungerbühler den mageren Informationen zur britischen HERF-Bankenerpressungstory gegenüber, erscheinen sowohl die Anzahl der Fälle als auch die Schadenssumme als nicht völlig unrealistisch.

Zum jetzigen Zeitpunkt kann man aber davon ausgehen, daß die Anwendung von "eletronischer Gewalt" gegen zivile Entitäten noch nicht stattgefunden hat. Die üblichen Trittbrettfahrer und Nachahmer dürften nicht lange auf sich warten lassen.

Die Herstellung von EMP/HERF-Geräten - soviel lässt sich den aus dem militärischen Bereich bekannt gewordenen Informationsfragmenten entnehmen - ist auf jeden Fall einfacher als die Produktion von Atombomben - schon allein, weil man keine kontrollierten Materiallien wie Uran benötigt. Aus dem erheblichen Mangel an zuverlässigen Informationen zum Thema resultieren die üblichen Probleme. Der "Sunday-Times"-Journalist wollte 30.000 Pfund für ein Video, daß eine solche Waffe im Einsatz zeigt. Für diese Summe lässt sich mühelos ein Video produzieren, daß so aussieht, als ob. Offenbar hat der gute Mann ob der schönen Story den Blick für die Realitäten etwas verloren.

frank@ccc.de



Buchbesprechung

„Die Datenmafia"

Für alle Freunde von Verschwörungstheorien und Realitätsabgleichen ist die „Datenmafia" wie geschaffen. Obwohl das Buch dank populärwissenschaftlicher Formulierungen (siehe Titel) auch für normale Menschen verständlich ist, erweitert es auch das Hackerhirn um eine Dimension.

Die Hintergründe geheimdienstlicher Tätigkeit, Verstrickungen mit Firmen und Softwarehäusern wird hier im Detail anhand des Beispiels „Promis" erläutert.

Anfang der 80er Jahre brachte die amerikanische Firma „Inslaw" eine Software namens PROMIS für Vax/VMS Systeme auf den Markt. PROMIS (Prosecutors Management Information System) erlaubte es Staatsanwaltschaften, Richtern, Polizei und Ermittlungsbehördern etc. nicht nur verschiedene Datenbanken zu verwalten, sondern vor allem diese miteinander abzugleichen und so aus verschiedenen (ungeklärten) Fällen die Gemeinsamkeiten zu ermitteln.

Soweit, so schlecht - die Firma wurde durch dubiose Vorfälle letztlich von amerikanischen Regierungsstellen in den Ruin getrieben, die Software mit einer Hintertür versehen und fortan über Geheimdienstkanäle an Regierungen in aller Welt verkauft. Die Dimension lässt auch ein stückweit die Hack´s der 80 Jahre im Umfeld des CCC und die Folgen in einem deutlicherem Licht sehen.

Die Geschichte von Promis hat u.a. durch einige umgebrachte recherchierende Journalisten und schließlich einem Ausschuss des amerikanischen Senats für einigen Wirbel gesorgt, ein technisches Detail nicht so sehr.

In dem Filmbeitrag „Hacker mit Geheimauftrag" den Egmont Koch vor einigen Wochen im ZDF zeigte kommt eine technische Delikatesse zur Sprache.

Michael Riconosciuto, der Mann, der die Hintertür in Promis für die NSA einbaute wurde - kurz nachdem er Aussagen vor eben diesem Kongressausschuß gemacht hatte - wegen Drogenhandels verhaftet und für satte 30 Jahre eingeknastet. Er berichtete schließlich, daß die NSA eines Tages die Grenzen der Promis-Hintertür erkannte. Denn die wirklich geheimen Informationen in Computern fremder Länder waren nicht vernetzt, sondern in standalone-Rechnern weggebunkert.

Um dennoch an die Datenbestände zu gelangen wurde ein Verfahren namens „Spreizbandstrahlung" ausgenutzt. Durch Erzeugung einer Abstrahlung auf den Adress/Datenbussen der Grossrechner (keine Hardwaremanipulation! Reines Wackeln von Strömen) wurde es anhand einer bestimmten Modulationsfrequenz möglich, die Daten wieder zu empfangen. Promis erhielt den Auftrag, den gesamten Datenbestand zyklisch auszusenden.

Zivile Nutzungsmöglichkeiten dieser Technologie (z.B. zur drahtlosen Vernetzung), die übrigens bereits Anfang der 70er Jahre (!) entwickelt wurde, gibt es bisher eher nicht.

Aber das ändert sich hoffentlich bald.

Egmont R. Koch und Jochen Sperber:
„Die Datenmafia" bei Rowohlt,
ISBN 3-498-06304-9

andy@ccc.de

Infos im Web:

Eidesstaatliche Erklärung von Riconosciuto vor dem Repräsentantenhaus und Parlamentarischer Untersuchungsbericht des Kongresses:
http://synside.sunnyside.com/cpsr/nii/sac/rights/inslaw

Verkauf von Promis:
http://www.copi.com/articles/inslaw-a.htm

Top Censored News Stories of 1991:
http://censored.sonoma.edu/ProjectCensored

Abt. Big Brother

Helm-Observation

Statt „Helm ab zum Gebet" heißt es bei der Polizei Helm auf zur Observation. Die neue Technik macht es möglich: im Beutel für die Gasmaske Camcorder und Akkus, im Helm eingebaut die Farbkamera mit automatischem Edelweißabgleich. Im Zentrum des Länderwappens vorn am Helm ein winziges Loch.

Das berichtete die Zeitschrift „Polizei heute".

Die Zeitschrift „DIE POLIZEI" schrieb am 20.09.1921: „Der bei Unruhen und pp. durch die Polizei „feldmäßig" aufgenommene Film wird ein wertvolles Abschreckungs-, Beweis- und Fahndungsmittel darstellen." (Nachdruck in HACKERBIBEL 1 S. 68, zZ vergriffen).

Polizeifilmaufnahmen gab es also schon 1911 !

Drei Augen sehen mehr als vier

„So berichten die Zeitungen von den kürzlichen Winzerunruhen und Meutereien in Frankreich, daß am 12. April (1911), als der Aufstand in der Champagne seinen Höhepunkt erreichte, in Ay (Dep. Marne) eine Reihe von kinematographischen Aufnahmen gemacht worden sind, auf denen die wilden Plünderungsszenen des Winzeraufstandes mit zweifelloser Genauigkeit und Klarheit dargestellt worden sind.

Jetzt hat sich das Gericht u. die Staatsanwaltschaft des zuständigen Gerichts in Reims in Gegenwart der Augenzeugen des Aufstands die Filme vorführen lassen, wodurch die schuldigen Plünderer und Rädelsführer mit Gewißheit & Leichtigkeit festgestellt & alsbald verhaftet werden konnten. Andererseits konnten auch einige der schon in U-Haft befindlichen Personen, die bisher ihre Teilnahme an den ...Unruhen leugneten, aber im kinematograph. Bilde erkannt wurden, so ihrerSchuld überführt werden.

... Zu diesen (polizeilichen) Hilfsmitteln gehört der kinematographische Aufnahmeapparat. ... Ich glaube wohl, daß eine gewisse, örtlich wirkende Abschreckungskraft im Aufnahmeapparat liegt, und daß er etwa wie die drohend auf unruhige Geister gerichtete Mündung eines Maschinengewehrs wirken kann."

85 Jahre nach Ersteinsatz des Polizeifilms in Frankreich hat das Braunschweiger Unternehmen Dieckhöner + Stiller Feingerätetechnik das Prinzip „Drei Augen sehen mehr als vier" erfolgreich abgeschlossen. Im allseits bewährten Schuberth-Polizeihelm P100A wurde wenige Millimeter über dem Visier Mikrofon und Farbkamera (330 000 Pixel) integriert.

Die Colorkamera ist komplett in den Helm integriert und so versteckt im Länderwappen. daß sie auch beim mehrmaligen Hinsehen kaum zu erkennen ist (Foto links). Die Aufnahmewinkel betragen 52 Grad vertikal und 72 Grad horizontal (Foto links oben).

Das winzige Loch für das Objektiv ist mitten im Länderwappen.

Der Aufzeichnungswinkel liegt bei 52 Grad vertikal und 72 Grad horizontal.

Aufgezeichnet wird auf einen modifizierten Camcorder von Sony, der samt 1,3 bis 3,2 mAh NiCd-Akku in der Gasmaskenbox der Berliner Auer-Gesellschaft steckt.

In einer weiteren Version „für ein anderes Einsatzfeld" kann ein Direktsender mit Universalantenne angeschlossen werden.

Das birgt jedoch für die Polizei das Risiko, daß - fernmeldejurologisch formuliert - „Andere" mitschneiden und zB die bei der Hamburger Polizei „irgendwie" gelöschten Beweismittelbänder in Fällen wie beim amtlich verprügelten Journalisten Oliver Neß „Nebenwirkungen" haben könnten durch Auftauchen „Anderer" Aufnahmen MIT den gelöschten Szenen.

Auch Filmmotive aus Polizeihubschrauberbersicht können bekanntlich mitgeschnitten werden, wenn zur ZF-Verschiebung im C-Band ein Astra-1-D-Konverter benutzt wird.

Die Datenschleuder bemüht sich um die Überlassung eines Testgerätesatzes zur u.a. Dokumentation von Fahrradfahrten durch die Stadt; evtl. beteiligt sich der Fahrradkurier Fritz Teufel am Test ;-)

Wau Holland

Sicherheitssimulation

Profitisierung der Polizei

Am 10.07.96 hat sich der Alterspräsident des Chaos Computer Club beim Bundeskriminalamt gemeldet und die Unterlagen einer öffentlichen Ausschreibung für ein Forschungsprojekt angefordert (und bis heute nicht erhalten). Das Thema der empirisch-kriminologischen Analyse:

„Möglichkeiten der Privatisierung von Aufgabenfeldern der Polizei mit Auswirkungen auf das Sicherheitsgefühl der Bevölkerung".

Der Impuls, beim BKA ein Angebot abzugeben für eine Studie, geht aus von der Gruppe um den CCC, die vor 11 Jahren eine Studie für den deutschen Bundestag über Computereinsatz durchführte. Immerhin hat diese Studie bei den Bonner Grünen bewirkt, daß sie 10 Jahre später nicht mehr grundsätzlich GEGEN Computer waren (es könnte aber auch an anderen Faktoren gelegen haben, meint der Sätzer). Es bleibt zu hoffen, daß eine weitere Studie bei den Wiesbadener Grünen bewirkt, daß sie schneller als in zehn Jahren nicht alle Polizisten durch Computer ersetzen wollen.

Da zu befürchten ist, daß das BKA den Projektentwurf des CCC-Umfeldes ablehnen wird, aber diese Studie nicht nur für das deutsche Volk wichtig ist, werden einerseits schon jetzt Sponsoren für diese Studie gesucht und andererseits Mitarbeiter.

Schon vor Beginn der Studienarbeit können absehbare Ergebnisse berichtet werden:

- Die Privatisierung von Arbeitsbereichen führt schon jetzt zu einer schleichenden Profitisierung. So werden zunehmend Radarfallen nicht an Unfallschwerpunkten, sondern an Einnahmeschwerpunkten aufgestellt

- Der Ersatz von Polizisten durch Computer führt zu Besonderheiten, wie sie SPIEGEL 30/96 auf S. 47 am Beispiel Voice-Mail in der New Yorker Westside beschreibt. Dort wollte eine Anruferin telefonisch einen blutigen Überfall melden.

„**Originalton**: >*Sie haben die 24. Wache erreicht. Wenn Sie von einem Tastentelefon anrufen, drücken Sie bitte 1. Andere Anrufer bleiben bitte in der Leitung.*
(Anrufer drückt die 1)
Wenn Sie anrufen, um über ein gerade stattfindendes Verbrechen oder einen Notfall zu berichten, drücken Sie die 1. Sie werden dann mit dem Notruf 911 verbunden. Wenn Sie nicht über einen Notruf, sondern beispielsweise über eine Lärmbeschwerde sprechen wollen, drücken Sie jetzt die Null. Wenn Sie die Beschwerdestelle für Verkehrsunfälle erreichen wollen, drücken Sie die 2. Um einen Streifenbeamten zu erreichen, drücken Sie die 3. Für eine kommunale Auskunftsstelle drücken Sie die 4. Um einen Polizeibeamten zu erreichen, drücken Sie die 5. Für alle anderen polizeilichen Angelegenheiten drücken Sie die Null oder bleiben Sie einfach in der Leitung.<
Dann wird diese gesamte Ansage, immerhin über eine Minute lang, wiederholt. Schließlich sagt die Stimme aus der Box:
>*Tut mir leid, dieser Anschluß antwortet nicht. Wir bedauern, daß Sie Schwierigkeiten haben. Bitte versuchen Sie es später noch einmal. Goodbye.*<"

Soweit der SPIEGEL und das ist ebensowenig Satire wie die BKA-Studie.

Verräterisch ist im Titel ein Begriff, der das Anliegen auf den Punkt bringt: Sicherheits-G e f ü h l, also etwas rein subjektives. Auch dieser Aufruf zur Mitarbeit ist bitter und ernst. Die Kooperation beginnt sofort über den eMail-Verteiler mit der Adresse bka@ccc.de

Wau Holland

BKA

Bundeskriminalamt Öffentliche Ausschreibung

Das Bundeskriminalamt in Wiesbaden beabsichtigt, zum 15.10.1996 folgendes Forschungsprojekt zu vergeben:

„Möglichkeiten der Privatisierung von Aufgabenfeldern der Polizei mit Auswirkungen auf das Sicherheitsgefühl der Bevölkerung.

– Eine empirisch-kriminologische Analyse –"

Wissenschaftler und Forschungsinstitute aus Kriminologie und verwandten Wissenschaftsbereichen, deren Qualifizierung durch eine Liste mit einschlägigen Veröffentlichungen/vgl. Referenzen nachgewiesen werden muß, können Projektentwürfe einreichen.

Die Laufzeit des Projektes beträgt ca. 18 Monate.

Die Ausschreibungsunterlagen können beim

Bundeskriminalamt
Referat ZV 23
65173 Wiesbaden
Fax 06 11 / 55 51 94

bis 10.07.1996 angefordert werden.

Später eingehende Anfragen können nicht berücksichtigt werden.

Ende der Ausschreibung (Angebotsfrist) 14.06.1996 (Eingang im BKA). Der Auftrag wird bis 01.10.1996 erteilt (Zuschlagfrist).

Mit der Einreichung der Projektentwürfe unterliegt der Bewerber den Bestimmungen über nicht berücksichtigte Angebote gem. § 27 VOL/A.

Kurz am Schluß..

Hacker verursachen Decoderstreit

(c) wau - Nur hinter zugehaltener Bethand geben die Kontrahenten im Dekoderstreit für das Pay-TV zu, daß letztlich die Angst vor Hackern eine Einigung verhindert.

Denn wenn sich zwei auf ein „Common Interface" einigen, dann müssen sie das offenlegen. Und die Paranoiker bei Bertelsmann und Kirch befürchten, daß ihr Kryptokrempel nicht hackfest ist.

AOL auf Scientology-Stil

(c) Wau - Nachdem ein DV-Journalist in den USA in einer Fachzeitschrift kritisch über AOL berichtet hatte, wurde ihm der Zugang gekündigt. Da er nicht gegen irgendwelche Vertragspflichten verstoßen hatte, wollte er den Grund erfahren.

Die AOL-Anwälte: Kunden, denen wir kündigen, haben kein Recht, zu erfahren, warum. Mal abwarten, welche Journalisten beim STERN sich trauen, darüber zu berichten und sich mit ihrem Kollegen zu solidarisieren - oder ob sie alle die Hosen gestrichen voll mit einer wirtschaftlichen Verflechtung.

Nettikettekenntnis

Internet ist in aller Munde, aber Regeln und gewachsene Umgangsformen sind dem breiten Publikum kaum bekannt. Private Mailboxbetreiber bemühen sich seit Jahren, die „Newbies" mit Infos auf Papier - vor allem Nettiketten - zu versorgen. Der erste kommerzielle Betreiber, der sich bemüht hat, dem Massenpublikum die Netikette nahe zu bringen, war die vielgeliebte TELEKOM. Bereits auf der letzten Funkausstellung in Berlin verteilte sie in hoher Auflage die Netikette Version TELEKOM in gedruckter Form mit ihrer Werbung. In Btx kann sie als Telesoft geladen werden von 1046501330. Einfacher:

Von der Hauptübersicht *0# mit 50 zu „Alles über T-Online", dann mit 13 zu Internet. Zu „Netiquette - Der Knigge für's Internet" geht es mit 30 und da steht: „Die guten Sitten wurden uns von klein auf anerzogen und jeder weiß, wie man sich bei Freunden zu verhalten hat. Aber: >And're Länder - and're Sitten<. Um alle unter einen Hut zu bekommen, entstand dieses weltweit anerkannte Regelwerk der Internet-Nutzer. Bitte respektieren auch Sie diese Regeln. Als Telesoftware laden mit #"

Hier hat die TELEKOM die Nase vorn; andere Anbieter können davon lernen.

James Leander

Nichols

Dänischer Honorarkonsul in Birma

Verurteilt zu 3 Jahren verstarb er Juli '96 im Knast von Rangun. Sein „Verbrechen" war das ungenehmigte Betreiben eines Faxgerätes.

Wir sind traurig

und werden alles uns mögliche tun, um durch freiere Kommunikation Terror-Regimes zu beseitigen.

Hacker und Hackson aus aller Welt

Nachruf

Für und an Mookie

Ende Juni starb Mookie im Untersuchungsgefängnis. Er war auf eine Bahn gekommen, von der man sich nur schwer lösen kann.

Mokkie war mit harten Drogen (LSD, MDA) in Berührung gekommen, aber er hatte es geschafft und sich nach einem Horrortrip losgesagt.

Leider war die Staatsgewalt schneller und klagte ihn wegen Drogenhandels an..

Mookie tauchte das erste Mal auf dem Chaos Communication Congress 1992 auf.

Er übernahm sofort den ungeliebten Job der Fahrbereitschaft.

Auch in den nachfolgenden Jahren traf man ihn immer wieder beim Kongress als Chaosengel an.

Die Computerszene hatte ihn gepackt. Als er in Kiel lebte, betrieb er im Studentenwohnheim eine Mailbox, die reges Interesse hervorbrachte.

Ich habe Mookie erstmals auf dem CCC 1995 kennengelert. Auch hier zeichnete er sich wieder in vorbildlicher Weise als Chaosengel aus.

Nach dem Kongress erschien Mookie regelmässig in den Clubräumen und half bei Renovierung und Neuinstallation der Technik.

Mookie begann Referate und Kurse über EDV und Sicherheit zu halten, die sehr positiven Anklang fanden. Auch kümmerte er sich um das Chaos der Post und wollte den Job des Kassenwartes übernehmen.

Leider waren andere wichtige Dinge in seinem Leben fehlgeschlagen.

Er hatte seine Ausbildung als Gross- und Ausenhandelskaufman abgebrochen und war lange Zeit arbeitslos.

Eine neue Lehrstelle als EDV-Kaufmann konnte er nicht beginnen, da die Firma verkauft wurde. Er verstand es jedoch sich zu fangen und war dabei, sich einen neuen Ausbildungsplatz zu suchen.

Mookie, schade das es so kommen musste. Wir hatten tolle Pläne, die jetzt nicht mehr verwirklicht werden können.

„Mookie, wir vermissen Dich"

Tritt nicht auf die Bazonga.

Amok

Adressen

CCC Hamburg -
Treff jeden Dienstag ab 20 Uhr in den Clubräumen oder im griechischen Restaurant gegenüber. Schwenckestr. 85, D-20255 Hamburg - Achtung! Neue Rufnummer:
Tel. 040-401801-0, Fax. 040-4917689,
E-Mail: ccchh@ccc.de

CCC Berlin -
Treffen jeden Dienstag ab 20 Uhr in den Clubräumen, Neue Schönhause Strasse 20 (Vorderhaus, ganz oben), 10178 Berlin (zwischen Hackescher Markt und Alexanderplatz)
Tel. 030-283 5487 0, Fax. 030-283 5487 8,
E-Mail: cccbln@ccc.de

CCC Lübeck -
Treff am ersten und dritten Freitag im Monat um 19 Uhr im "Shorty's", Kronsforder Allee 3a. Briefpost: CCC-HL c/o Benno Fischer, Bugenhagenstr. 7, D-23568 Lübeck. Tel. 0451-3882220, Fax. 0451-3882221
E-Mail: ccc@ews.on-luebeck.de,
http://www.on-luebeck.de/bfischer/ccc.html

CCC Südthür -
Status zur Zeit unklar. Wau ist dort irgendwo. Briefpost: Wau Holland, Professor-Schmidt-Str. 3, D-98693 Illmenau

CCC Ulm -
Treff jeden Montag, 19 Uhr im Cafe Einstein an der Uni Ulm.Kontakt:
E-Mail: frank.kargl@rz.uni-ulm.de

2600 Magazine - the hackers quarterly
(amerikanische Hackerzeitschrift)
Overseas 30$ individual, $65 corporate. Back issues available at $25 per year. $30 per year overseas. Adress all subscription correspondenco to:2600 Subscribtion Dept., P.O. Box 752, Middle Island, NY 11953-0752
Tel. +1-516-751 2600, Fax. +1-516-474,2677

FoeBud -
Bielefelder: Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.
Treff jeden Dienstag um 19:30 im CafeWissensdurst (ehemals Spinnerei) in der Heeperstr. 64. Dort Telefon Dienstag abends 0521-62339.
Monatliche "Public Domain" Veranstaltung, Info in der Bionic-Mailbox.
Foebud, Marktstr. 18, D-33602 Bielefeld,
Tel. 0521-175254, Fax. 0521-61172
Mailbox Bionic 0521-68000,
E-Mail: zentrale@bionic.zerberus.de

SUECRATES -
Stuttgarter Computerrunde mit Zeitschrift d'Hacketse. Kontakt: T. Schuster, Im Feuerhaupt 19, D-70794 Filderstadt,
E-Mail: norman@delos.stgt.sub.org

Engagierte Computer ExpertInnen -
Schweiz. Info: Postfach 168, A-1015 Wien

keine wirkliche Anzeige

Anhäufung kreativer Menschen sucht unter dem Motto
„Arbeit gibt es genug, der Lohnanspruch entscheidet."

engagierte MitarbeiterInnen (bürokratisch aber chaoskompatibel)

für
Mitgliedsverwaltung, Aboversand, Kontoführung, Abwasch, Telefondienst, leichte und schwere Reinigungsarbeiten, Betreuung hochbegabter aber sozial extraterristischer Jugendlicher in verschiedenen Alterslagen, Sonstiges.
Verdienst garantiert, Einkommen nicht.
Interessierte melden sich bitte beim CCC e.V.

Absender, Bezugs- und Bestellanschrift:

Chaos Computer Club e.V.
Schwenckestr. 85
D-20255 Hamburg
Tel. 040 - 401 801 - 0
Fax. 040 - 491 76 89

Name

Strasse

PLZ/Ort

Tel/E-Mail

---

o Ich möchte erstmal mehr wissen; bitte schickt mir die Satzung des CCC e.V. und einen Mitgliedsantrag; 5.- DM lege ich in Briefmarken bei.

o Ich will Mitglied werden, kann aber nur den ermässigten Jahresbeitrag von 60.- DM im Jahr zahlen. Zusammen mit der einmaligen Verwaltungspauschale von 20.- DM zahle ich also erstmal 80.- DM, zahlungsweise siehe unten.

o Ich will Mitglied werden und kann den normalen Jahresbeitrag von 120.- DM zahlen. Inkl. einmaliger Verwaltungspauschale also 140. -DM, zahlweise siehe unten.

o Ich will Mitglied werden und kann einen Förderjahresbeitrag von _____ DM zahlen. Diesen zahle ich hiermit zusammen mit der Verwaltungspauschale von 20.- DM.

o Ich möchte die Datenschleuder abonnieren; zum Normalpreis von 60.- DM für 8 Ausgaben.

o Ich möchte die Datenschleuder abonnieren, kann aber nur den ermässigten Preis von 30.-DM für 8 Ausgaben zahlen.

Die Kohle liegt o in bar o als Verrechnungsscheck o in Briefmarken bei bzw.

o wurde überwiesen am _____ auf das Kto. 59 90 90 - 201 bei der Postbank Hamburg BLZ 200 100 20 des Chaos Computer Club e.V.

Ort/Datum/Unterschrift _____

Bestellfetzen

Ab sofort Trennung von Bestellungen und Mitgliedsanträgen bzw. Abos. Dadurch geht beides schneller. Ggf. zweimal Name/Anschrift eintragen.

Preise gültig bis zur nächsten Ausgabe (DS56) - Oktober 1996

Literatur

_____05.00	DM	Doku zum Tod von „KGB"Hacker K.Koch
_____20.00	DM	Zerberus-Mailbox-BenutzerInnen Handbuch
_____29.80	DM	Deutsches PGP-Handbuch + aktuelle Version
_____25.00	DM	Vollständige Dokumentation des CCC'95

Alte Datenschleudern

_____50.00	DM	Alle Datenschleudern der Jahre 1984-1989
_____15.00	DM	Alle Datenschleudern des Jahres 1990
_____15.00	DM	Alle Datenschleudern des Jahres 1991
_____15.00	DM	Alle Datenschleudern des Jahres 1992
_____15.00	DM	Alle Datenschleudern des Jahres 1993
_____15.00	DM	Alle Datenschleudern des Jahres 1994
_____15.00	DM	Alle Datenschleudern des Jahres 1995

Aufkleber teilweise nur noch Restposten, solange Vorrat reicht.

_____03.33	DM	3 Aufkleber „Kabelsalat ist gesund"
_____05.00	DM	15 Aufkleber „Achtung Abhörgefahr" in grau
_____05.00	DM	Bogen m. Postknochen-Aufklebern

+ 05.00	DM	Portopauschale!

_____ Gesamtbetrag o liegt als V-Scheck o in Bar bei bzw.
o wurde am _____ überwiesen auf das Konto 59 90 90 - 201
bei der Posthank Hamburg (BLZ 200 100 20) des CCC e.V.

Name _____

Strass _____

PLZ, Ort _____